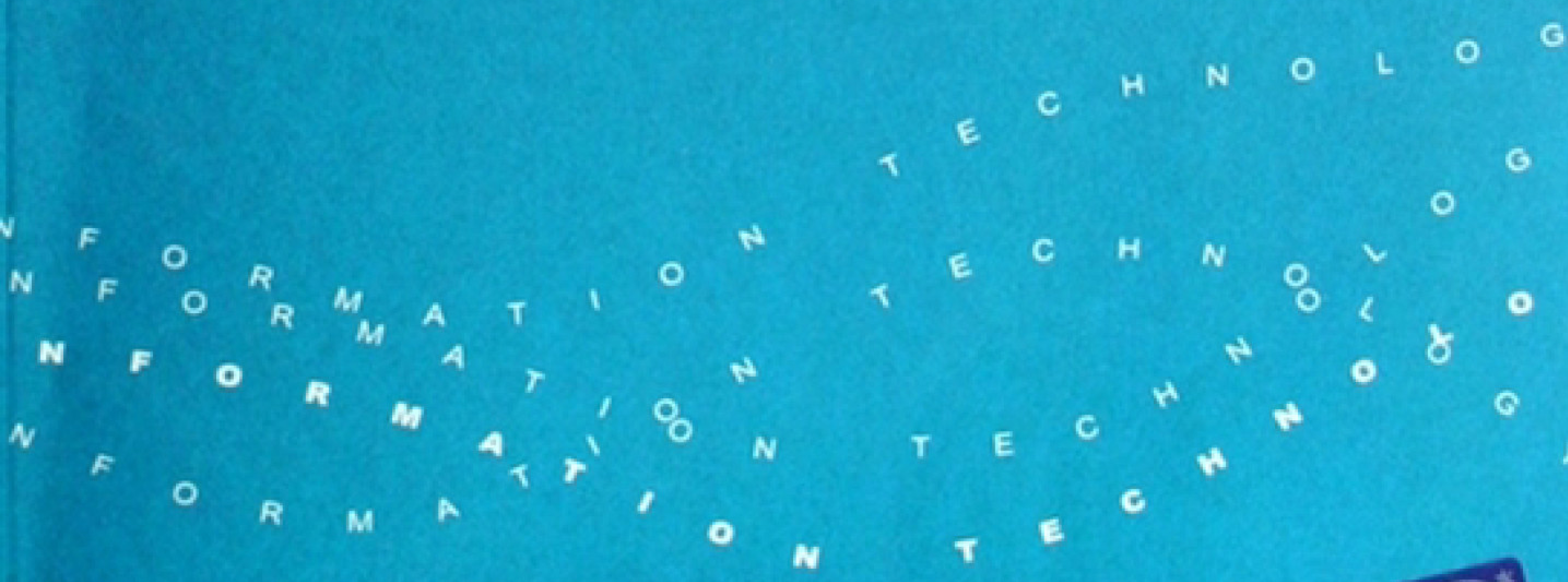
高等院校信息技术规划教材

# 计算机网络安全实用技术

符彦惟 等编著




清华大学出版社

高等院校信息技术规划教材

# 计算机网络安全实用技术

符彦惟　姜熙炯　郝培华　李军华　编著

清华大学出版社
北京

**内 容 简 介**

本书介绍计算机网络安全的基本原理和应用。全书共分8章，在概括性介绍网络安全基本工作原理的基础上，重点介绍局域网服务器操作系统、应用系统和个人计算机在互联网中如何保证安全运行。本书强调应用特色，并介绍网络安全的新技术，使读者学会应用、更好地理解和掌握实用的网络安全的技术。

本书可作为大学本科和大专非计算机应用专业有关课程的教材，也可作为广大计算机用户和网络管理员的参考书。



**图书在版编目（CIP）数据**

计算机网络安全实用技术/符彦惟等编著. —北京：清华大学出版社，2008.9
（高等院校信息技术规划教材）
ISBN 978-7-302-17966-5

Ⅰ.计…　Ⅱ.符…　Ⅲ.计算机网络－安全技术－高等学校－教材　Ⅳ.TP393.08

中国版本图书馆CIP数据核字(2008)第093453号

**责任编辑**：袁勤勇　赵晓宁
**责任校对**：白　蕾
**责任印制**：何　芉

**出版发行**：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　　编**：100084
**社 总 机**：010-62770175　　**邮　　购**：010-62786544
**投稿与读者服务**：010-62776969，c-service@tup.tsinghua.edu.cn
**质 量 反 馈**：010-62772015，zhiliang@tup.tsinghua.edu.cn
**印 刷 者**：北京市人民文学印刷厂
**装 订 者**：三河市新茂装订有限公司
**经　　销**：全国新华书店
**开　　本**：185×260　　**印　张**：27.75　　**字　数**：652千字
**版　　次**：2008年9月第1版　　**印　次**：2008年9月第1次印刷
**印　　数**：1～4000
**定　　价**：38.00元

---

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177转3103　　产品编号：022669-01

# 编委会名单

# 序 preface

在科教兴国方针的指引下，我国高等教育进入了一个新的历史发展时期，招生规模和在校生数量都有了大幅度的增长。我们在进行着世界上规模最大的高等教育。与此同时，对于高等教育的研究和认识也在不断深化。高等学校要明确自己的办学方向和办学特色，这既是不断提高高等教育水平的必然要求，更是高校不断发展和壮大必须首先考虑的问题。

教育部领导明确提出，高等教育应多元化，高等院校应实施分类分层次教学，这是高等教育大众化的必然结果，也是市场对人才需求的客观规律所致。因此要有相当部分的高等院校致力于培养应用型人才。此类院校在计算机教学中如何实现自己的培养目标，如何选择适用的应用型教材，已成为十分重要和迫切的任务。应用型人才的培养不能简单照搬研究型人才的培养模式，要在丰富的实践基础上认真总结，摸索新形势下的教学规律，在此基础上设计相关课程、改进教学方法，同时编写与之相适应的应用型教材。这一工作是非常艰巨的，也是非常有意义的。

在清华大学出版社的大力支持和配合下，应用型教材编委会于2003年成立。编委会汇集了众多高等院校的实践经验，并经过集中讨论和专家评审，遴选了一批优秀教材，希望能够通过这套教材的出版和使用，促进应用型人才培养的实践发展，为建立新的人才培养模式作出贡献。

我们编写应用型教材的主要出发点是：

1. 适应新形势下教育部对高等教育的要求以及市场对应用型人才的需求。

2. 计算机科学技术和信息技术发展迅速，教材内容和教学方式应与之相适应，适时地进行更新和改进。

3. 教育技术的发展对教材建设提出了更高的要求，教材将呈现

出纸介质出版物、电子课件以及网络学习环境等相互配合的立体化形态。

4. 根据不同的专业要求，突出应用，使理论与实践更加紧密结合。

以此为目标，我们将努力编写一套全新的、有实用价值的应用型计算机教材。经过参编教师的努力，第一批教材已经面世。教材将滚动式地不断更新、修正、提高，逐渐树立起自己的品牌。希望使用本系列教材的广大师生能对我们的教材提出宝贵的意见，共同建设具有应用型特色的精品教材。

朱　敏

2006 年 5 月

# 前言 foreword

在21世纪，计算机网络尤其是Internet技术已经改变了人们的生活、学习、工作乃至思维方式，但随之而来的各种有关网络安全问题也时时刻刻在困扰着网络上的每个用户和网络运行的管理者，病毒、黑客攻击几乎成了家常便饭，人们离不开网络，对网络是既爱又恨。所有这一切都源于网络的开放体系，造成了网络安全的脆弱。但是，我们不能因噎废食，既然我们的工作和生活离不开网络，那我们只能勇敢的面对，针对出现的各种威胁网络安全的行为，拿起自卫武器，来捍卫我们网络家园，为广大的网络用户营造一个安详的网络应用环境。

本书参考教学时数为32～48学时。全书共包括8章：第1章介绍计算机网络安全的一些基本概念、网络面临的各种安全威胁，使读者对计算机网络安全有一个全面的了解；第2章介绍了网络安全体系以及TCP/IP体系下的安全分析方法；第3章介绍了网络安全的策略以及个人用户和局域网的安全措施；第4章介绍了在目前广泛使用的Windows、UNIX、Linux三种操作系统安全策略的实现方法；第5章介绍了网络应用系统所采用的安全技术以及具体的实现方法；第6章介绍了黑客经常采用的攻击方法以及防范措施；第7章介绍了网络安全的整体构架；第8章介绍了典型行业网络安全解决方案的案例。

本书第1章由符彦惟、郝培华编写；第2章由姜熙炯编写；第3和第4章由姜熙炯、符彦惟编写；第5章由李军华、符彦惟编写；第6和第8章由符彦惟、郝培华编写，第7章由符彦惟编写。全书由符彦惟主编，并随后统编、定稿。

由于计算机网络安全技术发展非常迅速，涉及的知识面广，加之作者水平有限，书中难免有错漏之处，欢迎广大读者批评指正。编写过程中参考了国内外相关教材，并得到了锐捷网络公司的大力支持，在此一并表示诚挚的感谢。

编　者

2008年1月

# 目录

Contents

# 第1章 chapter 1

# 计算机网络安全概述

当今人们在享受计算机网络给工作和生活带来的各种便利的同时，也承受着脆弱的计算机网络安全体系带来的困扰和损失。网络上泛滥的病毒、黑客攻击已经成为无法回避而且有必须面对的问题。随着计算机网络的发展，人们对它的依赖性也加强了，不可能为了逃避网络安全带来的各种弊端而放弃它。因此，只有积极面对，依靠计算机网络安全技术的发展，才能保证生活和工作中的损失能减少到最低程度。本书的目的就是让读者了解网络安全的概念，给读者提供一些目前各种计算机网络运行中所遇到的安全问题的解决方法，让读者成为网络安全管理的高手。

## 1.1 网络安全的概念

### 1.1.1 信任与网络安全

“安全”是损伤、损害的反义词，网络安全的含义是泛指网络环境下计算机系统中数据的损伤性变化（即网络环境下公开的数据和受保护的数据遭到破坏、篡改、泄露、删除等。形成上述结果的方法多种多样，也与多种因素有关）。造成损伤的机制非常复杂，这与网络的开放性有很大关系，而且与网络环境下的用户关系也很密切。因此，网络安全涉及很多学科分支，是一个开放性复杂问题，这也造成了网络安全定义的多样性。

网络安全从其本质上讲就是网络上的信息安全，它涉及的领域相当广泛。这是因为在目前的公用通信网络中存在各种各样的安全漏洞和威胁。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论，都是网络安全所要研究的领域。

网络安全通用的定义是指网络系统的硬件、软件及其系统中的数据受到保护，不会因偶然或者恶意的原因遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

从用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒允、篡改、抵赖等手段对用户的利益和隐私造成损害和侵犯，同时也希望当用户的信息保存在某个计算机系统上时，不会受到其他非法用户的非授权访问和破坏。

从网络运行和管理者的角度来说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等威胁，制止和防御来自网络“黑客”的攻击。

对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，防止其通过网络泄露，从而避免由于这类信息的泄密对社会产生危害，给国家造成巨大的经济损失。

从社会教育和意识形态角度来讲，网络上不健康的内容会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

因此，网络安全在不同的环境和应用中会得到不同的解释。

(1) 运行系统安全，即保证信息处理和传输系统的安全，包括计算机系统机房环境的保护，法律、政策的保护，计算机结构设计上的安全性考虑，硬件系统的可靠安全运行，计算机操作系统和应用软件的安全，数据库系统的安全，电磁信息泄漏的防护等。它侧重于保证系统正常的运行，避免因为系统的崩溃和损坏对系统存储、处理和传输的信息造成破坏和损失，避免由于电磁泄漏产生信息泄漏干扰他人(或受他人干扰)，本质上是保护系统的合法操作和正常运行。

(2) 网络上系统信息的安全，包括用户密码鉴别，用户存取权限控制，数据存取权限、方式控制，安全审计，安全问题跟踪，计算机病毒防治，数据加密等。

(3) 网络上信息传播的安全，即信息传播后果的安全，包括信息过滤，有害信息的过滤等。它侧重于防止和控制非法、有害的信息进行传播，避免公用通信网络上大量自由传输的信息失控，本质上是维护道德、法律或国家利益。

(4) 网络上信息内容的安全，即狭义的“信息安全”。它侧重于保护信息的保密性、真实性和完整性。避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为，本质上是保护用户的利益和隐私。

显而易见，网络安全与其所保护的信息对象有关。本质是在信息安全期内保证其在网络上流动时或者静态存放时不被非授权用户非法访问，但授权用户却可以访问。显然，网络安全、信息安全和系统安全的研究领域是相互交叉和紧密相连的。

本书所研究和讨论的网络安全的含义是通过各种计算机、网络、密码技术和信息安全技术，保护在公用通信网络中传输、交换和存储的信息的机密性、完整性和真实性，并对信息的传播及内容具有控制能力。

其实，对上述网络安全的含义进行通俗的解释，即是网络安全系统要解决的下列问题：谁会访问数据？用户可以访问什么资源？何时访问？这些问题的解决取决于所服务的特定组织，因为不同的组织对资源赋予的信任是不同的。

信任，就是人们按规定行事的可能性。人们对信任的理解通常是凭经验的。一般会认为，信任只能存在于两个彼此认识的人之间。信任一个完全陌生的人很难，但是如果经过一段时间的了解后，也许就能建立起信任关系。在网络环境中，对信任的理解会有所不同。如果确认某人被另一位受到信任的人信任，即便他是一位陌生人，也可能会信任他。这种认知成为了 SSL(secure sockets layer)和证书交换机制的基础。

定义信任这个名词之后，就可以如图 1-1 所示为系列资源标上信任等级，从最可信到

最不可信。

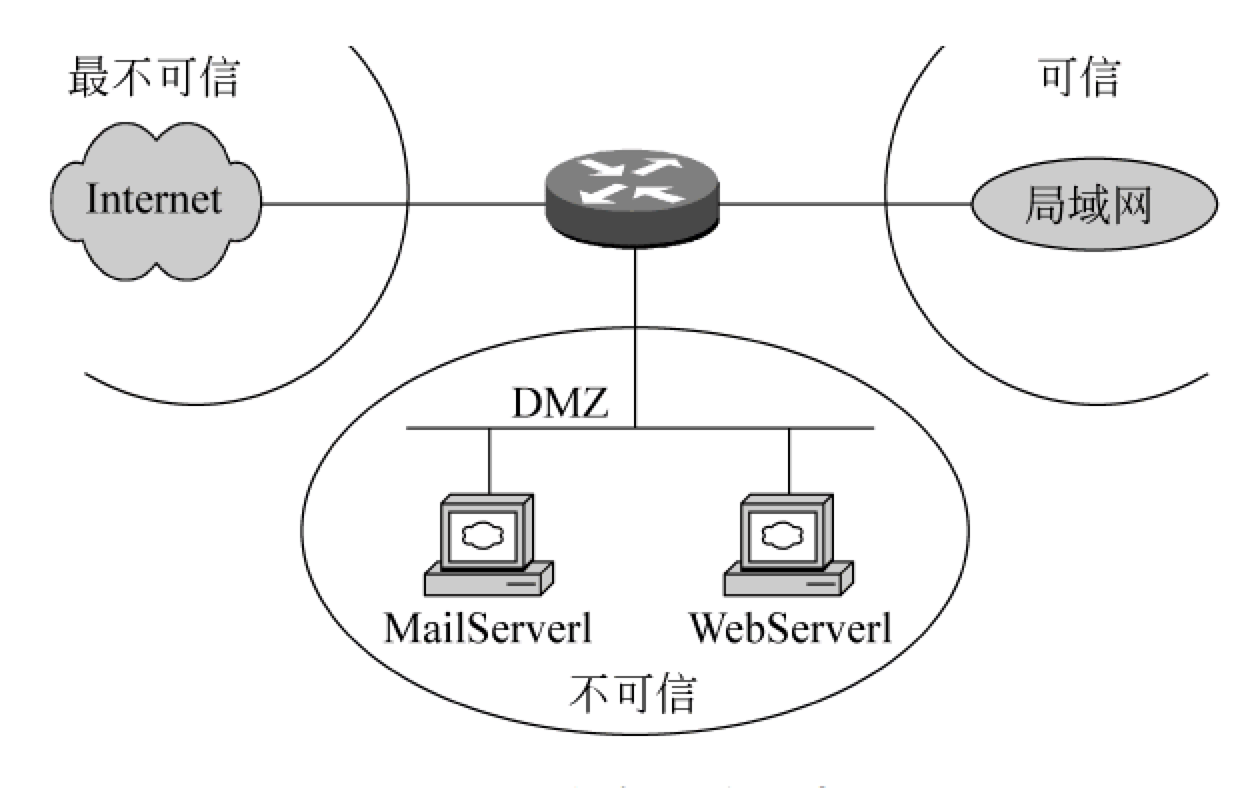



**图 1-1　安全区域示意图**

**1. 最可信(most trusted)**

对一个组织来说,最可信任的网络资源应该是内部服务器、域控制器和依附于网络的存储设备。这些设备只能被很少的确定的人员所访问。

**2. 不可信(less trusted)**

这类资源包括内部用户和远程的认证用户。为了工作所需,组织只在特定级别上信任该用户,包括内部和远程用户。即便为用户赋予了信任,有些人还是会利用密码来做违规操作。虽然大多数员工都是可信的,但因为滥用特权的情况仍然存在,才使得这个群体不得不被赋予不可信级别,而不是最不可信级别。

**3. 最不可信(least trusted)**

最不可信的资源和用户应该是 Internet 服务器和远程的未认证用户。永远不要信任一个 Internet 服务器,因为要确知隐藏其后的东西是很难的,这也是为什么要使用数字证书的原因。

## 1.1.2 网络安全标准

**1. OSI 安全体系结构的安全技术标准**

国际标准化组织在它所制定的国际标准 ISO 7498-2 中描述了开放系统互连基本参考模型(OSI)安全体系结构的 5 种安全服务,各服务的名称及用途如表 1-1 所示。

**2. 可信计算机评估标准(trusted computer system evaluation criteria,TCSEC)**

在美国,国际计算机安全中心(NCSC)负责建立可信计算机评估标准 TCSEC。TCSEC 指出了一些安全等级,被称做安全级别,它的范围从级别 A 到级别 D,其中 A 是

最高级别。高级别在低级别的基础上提供进一步的安全保护。级别 A、B 和 C 还为数字标明了子级别，各级别的名称及描述如表 1-2 所示。

**表 1-1　服务的名称及用途**

| 服　　务 | 用　　途 |
|---|---|
| 身份验证(Authentication) | 身份验证是证明用户及服务器身份的过程 |
| 访问控制(Access control) | 一旦用户身份被验证就发生访问控制，这个过程决定用户可以使用、浏览或改变哪些系统的资源 |
| 数据保密(Data confidentiality) | 这项服务通常使用加密技术保护数据免于未授权的泄露，可避免被动威胁 |
| 数据完整性(Data integrity) | 这项服务通过检验或维护信息的一致性，避免主动威胁 |
| 抗否认 (Non-reputation) | 否认是指否认参加全部或部分事务的能力。抗否认服务提供关于服务、过程或部分信息的起源证明或发送证明 |

**表 1-2　可信计算机系统评价准则**

| 级别 | 名　　称 | 描　　述 | 例　　子 |
|---|---|---|---|
| A1 | 可验证的安全设计 | 此级别要求严格的数学证明，证明系统不会危机安全 | Honeywll SCOMP |
| B3 | 安全域机制 | 提供数据隐藏和分层，保护层与层之间的所有交互信息 | Honeywll、Federal、Systems XTS-200 |
| B2 | 结构化安全保护 | 支持硬件保护，内存区域被虚拟分段，并进行严格保护 | XENIX、Honeywll MULTICS |
| B1 | 标号安全保护 | 除 C2 的保护级别外，把用户隔离成各个单元以提供进一步的保护 | AT&T System Ⅴ |
| C2 | 访问控制保护 | 以用户为单位的存储控制，广泛的审计和跟踪，对资源、数据、文件和进程提供系统级别的保护 | Windows 2000、UNIX |
| C1 | 选择的安全保护 | 用户与数据分离，不区分用户群，以用户组为单位 | 早期的 UNIX |
| D | 最小保护 | 无内在的安全保护 | MS-DOS |

### 3. 我国计算机安全等级划分与相关标准

对信息系统和安全产品的安全性评估事关国家和社会安全，任何国家不会轻易相信和接受由别的国家所作的评估结果。没有一个国家会把事关本国安全利益的信息安全产品和系统的安全可信性建立在别人的评估标准、评估体系和评估结果上。为保险起见，通常要通过本国标准的测试才被认为可靠。1989 年公安部在充分借鉴国际标准的前提下，开始设计和起草法律和标准，制定了《计算机信息系统安全保护等级划分准则》(以下简称为《准则》)的国家标准，并于 1999 年 9 月 13 日由国家质量技术监督局审查通过并正式批准发布，已于 2001 年 1 月 1 日执行。

《准则》将计算机信息系统安全保护能力划分为 5 个等级，计算机信息系统安全能力随着安全保护等级的增高，逐渐增强。各级别的描述如表 1-3 所示。

表 1-3 我国计算机系统安全准则等级

| 等级 | 名称 | 描述 |
|---|---|---|
| 第一级 | 用户自主保护级 | 它的安全保护机制使用户具备自主安全保护的能力,保护用户的信息免受非法的读写破坏 |
| 第二级 | 系统审计保护级 | 除具备第一级所有的安全保护功能外,要求创建和维护访问的审计跟踪记录,使所有的用户对自己行为的合法性负责 |
| 第三级 | 安全标记保护级 | 除具备前一级所有的安全保护功能外,还要求以访问对象标记的安全级别限制访问者的访问权限,实现对访问对象的强制访问 |
| 第四级 | 结构化保护级 | 除具备前一级所有的安全保护功能外,还将安全保护机制划分为关键部分和非关键部分,对关键部分可直接控制访问者对访问对象的存取,从而加强系统的抗渗透能力 |
| 第五级 | 访问验证保护级 | 除具备前一级所有的安全保护功能外,还特别增设了访问验证功能,负责仲裁访问者对访问对象的所有访问活动 |

### 1.1.3 网络安全责任

很多人员都能在网络的安全建设中发挥作用,从高级管理者到日常用户。高级管理者负责推行安全策略,其准则是"依其言而行事,勿观其行而仿之(Do as I say, not as I do)",但是源自高级管理者的策略和规则往往会被忽视掉。如果想让用户参与到安全维护的工作中,就必须让其相信管理者是非常认真严肃的。用户不仅要意识到安全的存在,而且要知道不遵守规则可能导致的后果。最好的方式是提供短期安全培训讲座,大家可以提问题并进行讨论。另一种好的做法是在来往频繁的公共场所和使用场所张贴安全警示(例如,网吧或者机房)。

需要说明的是,政府现在在安全方面也扮演着重要的角色,针对诸如无线和 IP 语音通信这样一些新兴技术制定了法规并且建立了一套法律体系就是很好的表现,如美国政府就为安全决策建立了法律要求。

健康保险便利及责任法案(healthcare insurance portability and accountability act, HIPAA)限制了对带有个人身份信息的健康数据的披露。

金融服务业现代化法案(Gramm-Leach-Bliley Act,GLB)影响着美国的金融机构,要求其向客户披露隐私策略。

电子通信隐私法案(Electronic Communications Privacy Act,ECPA)规定了哪些人可以在什么条件下读取哪些人的电子邮件。

**注意**:以上列举的只可以作为一种参考,并不代表全部。

### 1.1.4 网络安全目标

网络安全的最终目标就是通过各种技术与管理手段实现网络信息系统的可靠性、保密性、完整性、有效性、可控性和拒绝否认性。可靠性(reliability)是所有信息系统正常运行的基本前提,通常指信息系统能够在规定的条件与时间内完成规定功能的特性。可控性(controllability)是指信息系统对信息内容和传输具有控制能力的特性。拒绝否认性

(no-repudiation)也称为不可抵赖性或不可否认性，是指通信双方不能抵赖或否认已完成的操作和承诺，利用数字签名能够防止通信双方否认曾经发送和接收信息的事实。在多数情况下，网络安全更侧重强调网络信息的保密性、完整性和有效性，即CIA。

**1. 保密性**

保密性(confidentiality)是指信息系统防止信息非法泄露的特性。信息只限于授权用户使用，保密性主要通过信息加密、身份认证、访问控制、安全通信协议等技术实现。信息加密是防止信息非法泄露的最基本手段。事实上，大多数网络安全防护系统都采用了基于密码的技术，密码一旦泄露，就意味着整个安全防护系统的全面崩溃。如果密码以明文形式传输，在网络上窃取密码是一件十分简单的事情。保护密码是防止信息泄露的关键，加密可以防止密码被盗。机密文件和重要电子邮件在Internet上传输也需要加密，加密后的文件和邮件如果被劫持，虽然多数加密算法是公开的，但由于没有正确密钥进行解密，劫持的密文仍然是不可读的。此外，机密文件即使不在网络上传输，也应该进行加密；否则窃取密码后就可以获得机密文件，而且对机密文件加密可以提供双重保护。

**2. 完整性**

完整性(integrity)是指信息未经授权不能改变的特性。完整性与保密性强调的侧重点不同，保密性强调信息不能非法泄露，而完整性强调信息在存储和传输过程中不能被偶然或蓄意修改、删除、伪造、添加、破坏或丢失，在存储和传输过程中必须保持原样。信息完整性表明了信息的可靠性、正确性、有效性和一致性，只有完整的信息才是可信任的信息。影响信息完整性的因素主要有硬件故障、软件故障、网络故障、灾害事件、入侵攻击和计算机病毒等。保障信息完整性的技术主要有安全通信协议、密码校验和数字签名等。实际上，数据备份是防范信息完整性遭到破坏时最有效的恢复手段。

**3. 有效性**

有效性(availability)是指信息资源容许授权用户按需访问的特性，是信息系统面向用户服务的安全特性。信息系统只有持续有效，授权用户才能随时随地根据自己的需要访问信息系统提供的服务。有效性在强调面向用户服务的同时，还必须进行身份认证与访问控制，只有合法用户才能访问限定权限的信息资源。一般而言，如果网络信息系统能够满足保密性、完整性和有效性三个安全目标，在通常意义下就可认为信息系统是安全的。

**注意**：CIA的反义词是泄露、篡改和拒绝，即DAD(disclosure，alteration和denial)。

网络管理的一个主要安全目标是衡量安全成本和获益。任何一个安全系统不可能绝对安全的，而任何系统的安全保护也不可能不计代价。因此，如果要衡量保护某个实体需要多少费用，无论是存在于网络或计算机中的数据，还是组织的其他资产，都需要考虑进行风险评估。一般来说，组织的资产会面临多种风险，包括设备故障、失窃、误用、病毒、缺陷。

评估了资产以及与之相关的风险之后,还需要确定风险出现的可能性。尽管有很多威胁可能会影响到应用系统,但并非所有的威胁都会出现在现实环境中。例如,住在地震多发地带附近,地震的可能性就很大,但住在几乎从没发生地震的地方就不存在这种问题。为此,必须实施切实的风险评估,以确定对于特定地方的特定资源风险的可能性。风险一年中出现的可能性确定之后,即可定义所谓的年度发生率(annualized rate of occurrence,ARO)。

一旦计算出了 ARO,就可以将其与资产关联的货币投入相比较。这代表了一旦风险出现会损失多少钱。ARO 包含了新设备的价格、替换设备所需的人工费用以及员工不能正常工作造成的损失。最终计算出的风险所示值被叫做单一所示期望(single loss expectancy,SLE)。

为了应对可能的风险,需要为风险发生的可能性做出预算。为此,可以用 ARO 乘以 SLE,得出年度所示期望(annual loss expectancy,ALE)。这里举个例子,一台 Web 服务器造成其瘫痪的可能性是 39%,这就是风险的 ARO。如果架设于这台服务器之上的电子商务站点 1 小时创造的价值是 10 万元,由于修复系统,该站点估计会停工两小时,风险损失就是 20 万元。除了这个损失,还有替换服务器所带来的成本,如果服务器价值 6 万元,就会将总成本增加到 26 万元,这就是风险的 SLE。将 ARO 与 SLE 相乘,就会得出需要为此风险做出的预算了。

## 1.2 网络漏洞及安全隐患

计算机网络的开放性以及黑客的攻击是造成网络不安全的主要原因,而利用网络结构缺陷而造成的漏洞是黑客能突破网络防护进入网络的主要手段之一。

科学家在设计网络之初就缺乏对安全性的总体构想和设计,所用的网络通信协议是建立在可信的环境之下。例如,TCP/IP 协议主要考虑的是网络互联,它缺乏对安全方面的考虑。这种基于地址的协议本身就会泄露密码,而且 TCP/IP 协议是完全公开的,其远程访问的功能使许多攻击者无须到现场就能够得手,连接的主机基于互相信任的原则。而这些性质使得网络更加不安全。

### 1.2.1 网络结构带来的风险和不安全因素

计算机网络的设计缺陷包括以下两方面的内容。

(1) 物理结构的设计缺陷。局域网采用广播式网络结构,所有主机发送的信息在同一个网络中的其他主机易监听;广域网和 Internet 上的中继设备(如路由器)可以监听所有网络之间转发的信息。

(2) 网络系统的漏洞、协议的缺陷与后门。一些网络协议(如 TCP/IP 协议)在实现上力求实效,而没有过多地考虑安全因素;网络操作系统过于庞大,存在致命的安全漏洞;网络公司为了达到某些目的,在系统中设有安全后门也造成网络安全的隐患。

### 1. 物理网络结构易被窃听

计算机网络按通信信道类型分为广播式网络和点对点网络，这两种网络都存在不安全问题。

1）广播式网络的安全问题

当今大多数局域网采用的是以太网方式，以太网上的所有设备都连在以太网总线上，它们共享同一个通信通道。以太网采用的是广播方式的通信，广播式通信网络的特点是在该种通信子网中只有一个公共通信信道，为所有节点共享使用，任一时刻只允许一个节点使用公用信道。当一个节点利用公共通信信道发送数据时，必须携带目的地址。网络上所有的设备都能接收到每一个信息包，网络上的设备通常将接收到的所有包都传给主机界面，在此选择计算机要接收的信息（如选择只有地址符合本站点的信息包才接收），并将其他的过滤掉。以太网最有效传递的是目标主机硬件，并不给发送者提供有关信息已收到的信息，即使目标计算机碰巧关机了，送给它的包自然丢失，但发送者并不会知道这一点。

很多网络（包括 Internet）其实就是把无数的局域网连起来形成一个大的网，然后再把大的网连成更大的网。虽然网络上的传输是点对点的，但一般网络上的主机都会处于一个局域网中。例如，清华开放实验室是一个局域网，它连到了校园网，又连到了中国教育科研网（CERNET），中国教育科研网又连接到国外。局域网（如以太网、令牌网）都是广播型网络，也就是说一台主机发布消息，网上任何一台机器都可以收到这个消息。在一般情况下，以太网卡在收到发往别人的消息时会自动丢弃消息，而不向上层传递消息。但以太网卡的接收模式可以设置成混合型（promiscuous），这样网卡就会捕捉所有的数据包，并把这些数据包向上传递。这就是为什么以太网可以被窃听，其实 FDDI、令牌网也存在这样的问题。

2）点对点网络的安全问题

Internet 和大部分广域网采用点对点方式通信，在该种类型网中，任何一段物理链路都唯一连接一对节点。如果不在同一段物理链路的一对节点要通信，必须通过其他节点进行分组转发。进行分组转发的节点就可以窃听。

在 Internet 上的信息容易被窃听和劫获的另一个原因是，当某人用一台主机和国外的主机进行通信时，它们之间互相发送的数据包是经过很多机器（如路由器）层层转发的。例如，用户在清华开放实验室的一台主机上访问 Hotmail 主机，用户的数据包要经过开放实验室的路由器、清华校园网的路由器和中国教育科研网上的路由器，然后从中国教育科研网的总出口出国，再经过很多网络和路由器才能到达 Hotmail 主机。具体要经过多少主机、路由器和网络，可以用一个网络调试工具查到，这个工具就是 tracert 命令。这个命令在各种操作系统中都有，如 Windows 95、Windows NT 和 UNIX，名字上可能会有所差异，但功能和实现上是一样的。Internet 的这种工作原理不仅节约了资源，而且简化了传输过程的实现，符合 TCP/IP 简单高效的宗旨，但这也给安全上带来了问题。当然用户不可能为了安全而放弃这种方法，因为这样做是不实际的，也是不必要的。用户所能做的应该是意识到这种问题，并以其他办法来提高安全性，如采用数据加密的方

法。回到安全这个主题上来,当黑客使用一台处于用户数据包传输路径上的主机时,他就可以窃听或劫持用户的数据包。例如,处于中国教育科研网出口的一台机器可以监听所有从这个网络出国的数据包。举一个简单的例子,在配有电话交换机的单位,单位里所有的电话都要经过单位的总机,如果总机并不是程控的,而是人工接线的,那么接线员极易窃听别人的电话,这就类似刚才讲的网络窃听。网络窃听可能是出于好奇,也可能是出于恶意。现在越来越多的黑客不再是喜欢破坏公物的人,而是商业间谍,所以网络安全是把 Internet 真正推向商业化所必须要考虑和解决的问题。

3) 传输线路质量与安全问题

尽管在同轴电缆、微波或卫星通信中要窃听其中指定一路的信息是很困难的,但是从安全的角度来说,没有绝对安全的通信线路。

同时,无论采用何种传输线路,当线路的通信质量不好时,将直接影响联网效果,严重的时候甚至导致网络中断。例如,以市内电话线路作为传输线路时,主要电气指标如直流电气性能指标(环阻、绝缘电阻);交流特性(线路衰耗、线路衰耗交流频率特征);交流特性阻抗的好坏直接影响网络通信质量。当通信线路中断时,计算机网络也就中断了,这种情况还比较明显。而当线路时通时断、线路衰耗大或杂音严重时,问题就不那么明显,但是对通信网络的影响却是相当大,可能会严重地危害通信数据的完整性。为保证好的通信质量和网络效果,就必须要有合格的传输线路,如在干线电缆中应尽量挑选最好的线作为计算机联网专线,以得到最佳的效果。

### 2. TCT/IP 网络协议的设计缺陷

网络通信的基础是协议。TCP/IP 协议是目前国际上最流行的网络协议,该协议在实现上因力求实效,而没有考虑安全因素。因为如果考虑安全因素太多,将会增大代码量,从而会降低 TCP/IP 的运行效率,所以说 TCP/IP 本身在设计上就是不安全的。

下面是现存的 TCP/IP 协议的一些安全缺陷。

1) 容易被窃听和欺骗

在 Internet 上大多数的流量是没有加密的,如电子邮件密码、文件传输等很容易被监听和劫持,可以实现这些行为的工具很多,而且这些工具在网上是免费提供的。

2) 脆弱的 TCP/IP 服务

很多基于 TCP/IP 的应用服务都在不同程度上存在着不安全的因素,这很容易被一些对 TCP/IP 十分了解的人所利用,一些新的处于测试阶段的服务存在着更多的安全缺陷。

3) 缺乏安全策略

许多站点在网络及防火墙配置上无意识地扩大了访问权限,忽视了这些权限可能会被内部人员滥用。黑客从一些服务中可以获得有用的信息,而网络维护人员却不知道应该禁止这种服务。

4) 配置的复杂性

访问控制的配置一般十分复杂,所以很容易被错误配置,从而给黑客以可乘之机。

除上面的 4 个问题外,还有 TCP/IP 协议是被公布于世的,了解它的人越多,被人破

坏的可能性也就越太。现在,银行之间在专用网上传输数据所用的协议都是保密的,这样就可以有效地防止入侵。对于 UNIX 和 Windows NT 等网络系统的安全问题,总体来说 Windows NT 要比 UNIX 安全,这并不是说 Windows NT 的没有安全问题和缺陷,而是因为 Windows NT 的源代码不公开,而 UNIX 的源代码是极易得到的。当然,人们不能把 TCP/IP 协议和其源代码保密,这样不利于 TCP/IP 网络的发展,但可以在其他方面采取一些措施来弥补它。

随着计算机网络的发展,计算机网络的功能和服务也越来越强,但这也带来了很多安全问题,像 Windows NT 这样的网络系统,代码庞大,安全漏洞多。而且由于系统本身不完善和“后门问题”,可以被黑客们利用借以侵入网络,给网络安全带来很多隐患。

### 1.2.2 计算机网络系统的漏洞

经常说,某某系统存在大量漏洞,黑客利用漏洞攻击了系统。到底什么是漏洞? 黑客是怎样利用漏洞攻击系统的? 漏洞的危害性有多大? 下面将讲述这些方面的内容。

#### 1. 漏洞的等级

广义的漏洞是指非法用户未经授权获得访问或提高其访问层次的硬件或软件特征。

漏洞就是某种形式的脆弱性。实际上漏洞可以是任何东西。许多用户非常熟悉的特殊的硬件或软件都存在漏洞:IBM 兼容机的 CMOS 密码在 CMOS 的电池供电不足、不能供电或被移走造成 CMOS 密码丢失是漏洞;操作系统、浏览器、TCP/IP、免费邮箱等也存在漏洞。每个平台无论是硬件还是软件都存在漏洞。

网络漏洞主要是指网络产品或系统存在的缺陷给网络带来的不安全因素,产生的主要原因是设计网络产品或系统时考虑不周到。

由于网络系统的复杂性,网络漏洞产生不可避免,现在主要做的是当发现网络漏洞后,应及时采取补救措施。

根据网络漏洞或脆弱性给系统带来危害性的大小,漏洞可分为允许拒绝服务的漏洞(C 类)、允许有限权限的本地用户未经授权提高其权限的漏洞(B 类)、允许外来团体(在远程主机上)未经授权访问网络的漏洞(A 类)等 3 级类型。

1) 允许拒绝服务的漏洞(C 类)

允许拒绝服务的漏洞属于 C 类,它不会破坏数据或使数据泄密,是不太重要的漏洞。

黑客利用这类漏洞进行攻击几乎总是基于操作系统的,也就是说,这些漏洞存在于网络操作系统中。当存在这种漏洞时,必须通过软件开发者或销售商的弥补予以纠正。

对于大的网络或站点,拒绝服务攻击只是有限的影响,最多不过是使人心烦而已。然而对于小的站点,可能会受到拒绝服务的重创。特别对于站点只是一台单独的机器(单独的邮件或新闻服务器)更是如此。

拒绝服务攻击是一个人或多个人利用 Internet 的核心协议 TCP/IP 的某些缺陷产生大量数据阻塞网络,使服务器死机或因服务器负担过重使系统拒绝正常用户对系统信息进行合法的访问。

2) 允许本地用户非法访问的漏洞(B 类)

B类漏洞是允许本地用户获得增加的未授权的访问,这种漏洞一般在多种平台的应用程序中发现。

一个很好的例子是众所周知的 Sendmail 问题。Sendmail 可能是世界上发送电子邮件最盛行的方法,这个程序一般在系统启动时作为例程初始化并且只要机器可用它就可用。在活动可用状态下,Sendmail(在端口25)侦听网络空间上的发送请求。

当 Sendmail 启动时,它一般要求检验用户的身份,只有 root 和与 root 相同权限的用户有权启动和维护 Sendmail 程序。然而根据 CERT 咨询处的 Sendmail DaemonVulnerability 报告:“很遗憾,由于一个代码错误,Sendmail 在例程模式下可以以一种绕过潜入的方式激活。当绕过检查后,任何本地用户都可以在例程下启动 Sendmail。另外在8.7版本中,在 Sendmail 收到一个 SIGHUP 信号时会重新启动。它通过使用 exec(2)系统调用重新执行自己来重新开始操作。重新执行作为 root 用户实现。通过控制 Sendmail 环境,用户可以用 root 权限让 Sendmail 运行一任意的程序。”因此,本地用户获得一种形式的 root 访问。这些漏洞是很常见的,差不多每月都发生一次。Sendmail 以这些漏洞而出名,但却不是唯一的现象(也不是 UNIX 自身的问题)。

像 Sendmail 这样的程序中的漏洞特别重要,因为这些程序对网上所有的用户都是可用的,所有用户都至少有使用 Sendmail 程序的基本权限。如果没有的话,他们没法发送邮件。因此 Sendmail 中的任何 bug 或漏洞都是十分危险的。

B类漏洞唯一令人欣慰的是有较大的可能检查出入侵者,特别是在入侵者没有经验的情况下更是如此。如果系统管理员运行了强有力的登录工具,入侵者还需要有较多的专业知识才能逃避检查。

大多数B类漏洞产生的原因是由应用程序中的一些缺陷引起的。有些常见的编程错误导致这种漏洞的产生,如缓冲区的溢出。有关缓冲区的溢出的问题将在后面的有关章节中介绍。

3) 允许过程用户未经授权访问的漏洞(A类)

A类漏洞是威胁性最大的一种漏洞。大多数的A类漏洞是由于较差的系统管理或设置有误造成的。

典型的设置错误(或设置失败)是网络系统提供的任何存放在驱动器上的例子脚本,即使在这些版本的系统文档中建议管理员删掉这些脚本。这种漏洞在网络上重现过无数次,包括那些在 Web 服务器版本中的文件。这些脚本有时会为来自网络空间的侵入者提供有限的访问权限甚至 root 的访问权限。如 test_cgi 文件的缺陷是允许来自网络空间的侵入者读取 CGI 目录下的文件。Novell 平台的一种 HTTP 服务器有一个称做 Convert.bas 的例子脚本。这个用 BASIC 编写的脚本,允许远程用户读取系统上的任何文件。

A类漏洞涉及的不仅是一个文件,有时它与脚本的解释方法有关。例如,Microsoft 的 Internet 信息服务器(IIS)包含一个允许任何远程用户执行任意命令的漏洞。由于 IIS 将所有.bat 或.cmd 后缀的文件与 cmd.exe 程序联系起来,所以危害性很大。如 JulianAssange(Strobe 的作者)所解释的:“第一个 Bug 允许用户访问与 wwwroot 目录在同一分区的任何文件(认为 IIS_user 可以读此文件)。它也允许与脚本目录在同一分

区的任意可执行文件的运行(认为 IIS_user 足以执行此文件)。如果 cmd.exe 文件能被执行,那么它也允许你执行任何命令,读取任意分区的任意文件(认为 IIS_user 可以读取并执行此文件)……遗憾的是 Netscape 通信和 Netscape 商业服务器也都有相类似的 Bug。对于 Netscape 服务器使用 BAT 或 CMD 文件作为 CGI 脚本则会发生类似的事情。”

很自然,A 类漏洞对系统造成了严重的威胁。在许多情况下,如果系统管理员只运行了很少日志的话,这些攻击可能不会被记录,使捉获更为困难。

很容易体会到为什么像扫描器这样的程序会成为安全性的重要部分,扫描器的重要目的是检查这些漏洞。因此,尽管安全性程序员把这些漏洞包含进他们的程序中作为检查的选择,但他们经常是在攻击者之后几个月才这样做(某些漏洞,比如说允许拒绝服务的 synflooding 漏洞不容易弥补,目前系统管理员必须得学会在这些不尽人意的漏洞下工作)。

使形势更为困难的是非 UNIX 平台的漏洞要花更多的时间才会表现出来。例如,许多 Windows NT/2000 的系统管理员不运行重要的日志文件。因为报告漏洞,必须有漏洞存在的证据。另外,新的系统管理员(在 IBM 兼容机中,这样的管理员占很大比例)并没有对文档和报告安全性事故做好准备。这意味着漏洞出现后,从测试、重建测试环境及最后加入到扫描器前的时间被浪费了。

### 2. 系统安全漏洞

一个网络系统不仅包含了各种交换机、路由器、安全设备和服务器等硬件设备,还包含了各种操作系统、服务器软件、数据库系统以及应用软件等软件系统,系统结构十分复杂。从系统安全角度分析,任何一个部分要想做到万无一失都是非常困难的,任何一个疏漏都有可能导致安全漏洞,给攻击者造成可乘之机,带来严重的后果。然而,在大多数情况下,一个网络系统建立起来后,并不知道系统是否存在安全漏洞,往往不做任何的系统安全性测试和检测,只在发生网络攻击事件并造成严重的后果后,才意识到安全漏洞的危害性。根据美国联邦调查局的统计,世界上所发生的网络攻击事件中,80%以上是因为系统存在安全漏洞被内部或外部攻击者利用而造成的。

从网络攻击的角度来分析,常见的网络攻击方法可分成如下几种类型:扫描、探测、数据包窃听、拒绝服务、获取用户账户、获取超级用户权限、利用信任关系以及恶意代码(如特洛伊木马、病毒、蠕虫等)等。攻击者入侵网络系统主要采用两种基本方法:社会工程和技术手段。基于社会工程的入侵方法是攻击者通过欺骗手法引诱用户说出他们的密码,然后通过密码轻易地入侵网络系统。基于技术手段的入侵方法是攻击者利用系统设计、配置和管理中的漏洞来入侵系统。技术手段入侵主要有下述几种。

1) 潜在的安全漏洞

任何一种软件系统都或多或少地存在着安全漏洞。在当前的技术条件下,发现和修补一个系统所有安全漏洞是十分困难的,也是不可能的。一个系统可能存在的安全漏洞主要集中在如下几个方面。

(1) 密码漏洞:通过破译操作系统的密码而入侵系统是常用的攻击方法,使用一些

密码破译工具可以扫描 Windows NT 的密码文件。任何不及时更新密码的系统,都容易受到攻击。

(2) 软件漏洞:在 UNIX 中,NFS、NIS、Sendmail、Rlogin 和 Rsh 等程序都存在着一定的安全漏洞,容易受到攻击。

(3) 协议漏洞:利用协议漏洞也是常见的攻击方法。例如,IMAP 和 POP3 协议一定要在 UNIX 系统根目录下运行,攻击者可以利用这一漏洞发动对 IMAP 的攻击,破坏系统的根目录,从而取得超级用户的特权。

(4) 缓冲区溢出:这是最容易被攻击者利用的系统漏洞(下面详细讨论)。

(5) 拒绝服务:拒绝服务(DoS)攻击是通过产生大量虚假的数据包来耗尽目标系统的资源,如 CPU 周期、内存和磁盘空间、通信带宽等,使系统无法处理正常的服务,直到因为过载而崩溃。典型的 DoS 攻击有 SYN flood、FIN flood、ICMP flood、UDP flood 等。虚假的数据包还会使一些基于"失效开放"策略的入侵检测系统产生拒绝服务。所谓"失效开放"是指系统在失效前不会拒绝访问、由于虚假的数据包会诱使这种"失效开放"系统去回击那些并未发生的攻击,结果阻塞了合法的请求或是断开合法的连接,最终导致系统拒绝服务。

(6) 恶意代码:恶意代码是一组诸如病毒或蠕虫这样的破坏性程序,包括如下几个类型。

病毒(virus)——病毒是一组能够附着在程序、磁盘或计算机内存中以便自我繁殖的代码。病毒能够携带一个实施特定活动的有效载荷,从显示一则消息到删除一个计算机硬盘,活动范围非常广泛。

蠕虫(worm)——和病毒类似,蠕虫也可以自我复制。蠕虫能够利用电子邮件和网络设施来扩散并且创建新的复制。

特洛伊木马(Trojan horse)——特洛伊木马没有自我复制能力,它的特点是伪装成一个实用工具或者一个可爱的游戏,诱使用户将其安装在 PC 或者服务器上。

间谍件(spyware)——这是一类采集用户信息并发送到某个集中站点的软件。著名的音乐共享程序 Kazaa 上面就附着了一个间谍件,在它的用户许可协议中明确提到,如果用户接受其协议,就等于允许安装它所提供的间谍件并发出个人用户信息。

恶作剧(hoax)——这是一类特殊的恶意代码,它实际上并不包含任何代码,只是利用了用户的轻信而散播。这些东西通常都会使用一些带有感情色彩的主题,比如"孩子的最近一个愿望"。任何请求将同一个复制转发给其他熟人的电子邮件消息,都可以被认为是一类恶作剧。

脚本小子(scriptkiddies)——脚本小子是黑客的分支,他们通常会利用别人提供的脚本程序来破解特定系统上的某个安全漏洞。

2) 可利用的系统工具

很多系统都提供了用于改进系统管理和服务质量的系统工具,但这些系统工具同时也可能被攻击者利用,进行非法收集信息,为攻击打开方便之门。

(1) Windows NT NBTSTAT 命令:系统管理员使用该命令获取远程节点信息,但攻击者也可用该命令收集对系统有威胁性的信息。例如,网络管理员的身份信息、

NetBIOS 名、IIS 名以及用户名等。这些信息可以用来破译密码。

(2) Portscan 工具：系统管理员使用该工具检查系统的活动端口以及这些端口所提供的服务，攻击者也可出于同一目的而使用这一工具。

(3) 数据包窃听器(packet sniffer)：系统管理员使用该工具监控和分发数据包，以便找出网络的潜在问题。攻击者可以利用该工具截获流经网络的数据包，这些数据包中可能包含有未加密的密码和其他敏感信息，然后利用这些数据来攻击网络。

3) 不正确的系统设置

不正确的系统设置也是造成安全隐患的一个重要因素。当发现安全漏洞时，管理员应仔细分析危险程度，并马上采取补救措施。有时虽然已经对系统进行了维护，对软件进行了更新或升级，但由于一些网络设备(如路由器、防火墙等)配置过于复杂，系统还可能会出现新的安全漏洞。因此，及时和有效地改变系统设置可以大大降低系统所承受的风险。

4) 不完善的系统设计

在不重视信息安全情况下所设计出来的软件系统是很不安全的，难以抵御网络攻击。在网络系统设计时，应当从底层着手来建立安全的系统架构，使系统能够提供有效的安全服务和管理。不完善的网络系统和软件设计将会给攻击者带来可乘之机。在很多发表的安全漏洞报告中都指出：在输入检查不完全时，cgi-bin 是非常脆弱的。攻击者可以利用这一漏洞发动 DoS 攻击，非法访问敏感信息或是篡改 Web 服务器的内容。

**3. 漏洞类型**

攻击者在实施网络攻击时，首先要寻找一个网络系统的各种安全漏洞，然后分析和利用这些安全漏洞来入侵网络系统。系统安全漏洞大致可分成如下几类。

(1) 软件漏洞：任何一种软件系统都或多或少存在一定的脆弱性，安全漏洞可以看做是已知的系统脆弱性。例如，一些程序只要接收到一些异常或者超长的数据和参数，就会导致缓冲区溢出。这是因为很多软件在设计时忽略或者很少考虑安全性问题，即使在软件设计中考虑了安全性，也往往因为开发人员缺乏安全培训或没有安全经验而造成安全漏洞。这种安全漏洞可以分为两种：一是由于操作系统本身设计缺陷带来的安全漏洞，这种漏洞将被运行在该系统上的应用程序所继承；二是应用软件程序的安全漏洞，这种漏洞最常见，更需要引起广泛的关注。

(2) 结构漏洞：在一些网络系统中忽略了网络安全问题，没有采取有效的网络安全措施，使网络系统处于不设防状态。在一些重要网段中，交换机和集线器等网络设备设置不当，造成网络流量被监听和获取。

(3) 配置漏洞：在一些网络系统中忽略了安全策略的制定，即使采取了一定的网络安全措施，但由于系统的安全配置不合理或不完整，安全机制并没有发挥作用。在网络系统发生变化后，由于没有及时更改系统的安全配置而造成安全漏洞。

(4) 管理漏洞：指因网络管理员的疏漏和麻痹造成的安全漏洞。例如，管理员密码太短或长期不更换，造成密码攻击。两台服务器共用同一个用户名和密码，如果一个服务器被入侵，则另一个服务器也不能幸免。

（5）信任漏洞：一个系统过分地信任某个外来合作者的机器，一旦这个合作者的机器被入侵，则整个系统的安全将受到严重的威胁。

人们经常会犯一些安全错误，如认定攻击总是来自组织外部，就像很多公司在其建筑物之外构筑了坚固的围墙，但其内部的门却都不加锁一样。下面列举的是组织内部常见的一些由于管理和信任漏洞造成的威胁。

受认证的用户——这些用户经过认证和授权，可以使用网络中特定的资源。他们往往会利用已经获得的访问权限去得到诸如工资单或个人记录这样的机密数据。

非授权用户——在组织内部，用户有时候会安装一些未被授权的程序和插件，这等于开放了很多漏洞。

未打补丁的软件——保持软件及时更新或打补丁是非常重要的。一旦一个软件漏洞被识别，供应商会向相关客户提供更新件。经常检查并更新补丁是很好习惯，特别是对浏览器和操作系统。如果运行的是微软的操作系统。例如，Windows 2000，下面的链接是有用的。

http://www.microsoft.com/windows2000/downloads/critical/default.asp

这个 URL 链接指向列举了所有可供下载的关键更新，特别针对微软操作系统的操作过程也适用于 Web 浏览器和其他 PC 中使用的程序。此外，Internet 上还有很多邮件列表经常会发布有关更新补丁的最新消息，例如，下面两个网址的内容。

http://www.truesecure.com 和 http://www.csoonline.com

从这些安全漏洞来看，既有技术因素，也有管理因素和人员因素。实际上，攻击者正是分析了与目标系统相关的技术因素、管理因素和人员因素后，寻找到其中的安全漏洞来入侵系统的。因此，阻塞安全漏洞必须从技术手段、管理制度和人员培训等方面采取有效的措施。安全漏洞扫描技术是一种技术手段，但只靠技术手段是不够的，还必须从制定安全管理制度、培养安全管理人员和加强安全防范意识教育等方面来提高网络系统的安全防范能力和水平。

## 1.2.3 计算机网络技术的安全隐患

计算机网络的安全隐患是多方面的。从网络组成结构上分，有计算机信息系统的和有通信设备、设施的；从内容上分，有技术上的和管理上的。从技术上来看，主要有以下几个方面。

### 1. 网络系统软件自身的安全问题

网络系统软件的自身安全与否直接关系到网络的安全。网络系统软件的安全功能较少或不全，以及系统设计时的疏忽或考虑不周而留下的“破绽”都等于给危害网络安全的人或事留下许多“后门”。例如，美国微软公司就经常针对已发现的系统“破绽”发布“补丁”程序。同时，在同一系统软件中，低版本往往比高版本在安全性能方面差许多，所以在服务器上要注意尽量使用高版本的操作系统，并使用系统软件所能提供的最高安全级别。另外，值得注意的是操作系统的许多默认值都已经被黑客们盯上了，往往被用来作为侵入网络的突破口，所以应尽量避免使用系统默认值。此外，还要注意的有以下

几项。

（1）操作系统的体系结构造成其本身是不安全的，这也是计算机系统不安全的根本原因之一。操作系统的程序是可以动态连接的，包括I/O的驱动程序与系统服务都可以采用打“补丁”的方式进行动态连接。许多UNIX操作系统版本的升级、开发都是采用打“补丁”的方式进行的。这种方式既然厂商可以使用，那么黑客也可以使用，同时这种动态连接也成为计算机病毒产生的好环境。

（2）操作系统的一些功能，例如，在网络上传输文件的功能，包括支持传输可以执行的文件映像，即可在网络上加载程序等，必然带来一些不安全因素。

（3）操作系统不安全的另一原因在于它可以创建进程，甚至支持在网络的节点上进行远程进程的创建与激活，更重要的是被创建的进程可以继承创建进程的权力。这一点与可在网络上加载程序结合起来就构成了可以在远端服务器上安装“间谍”软件的条件。若再把这种间谍软件以打补丁的方式“打”在一个合法的用户上，尤其是“打”在一个特权用户上，系统进程与作业监视程序就都无法监测这些黑客和间谍软件的存在。

（4）操作系统运行时，一些系统进程总在等待一些条件的出现，一旦满足要求的条件出现，程序便继续运行下去，这都是黑客可以利用的。

（5）操作系统要安排无密码入口，这原本是为系统开发人员提供的便捷入口，但也是黑客的通道。另外，操作系统还有隐蔽信道。

（6）Internet和Intranet使用的TCP/IP（传输控制协议/网际协议）以及FTP（文件传输协议）、E-mail（电子邮件）、RPC（远程程序通信规则）、NFS（网络文件系统）等都包含许多不安全的因素，存在着许多漏洞。

### 2. 网络系统中数据库的安全设计问题

网络中的信息数据是存放在计算机数据库中的，供不同的用户共享。数据库存在着不安全性和危险性，因为在数据库系统中存放着大量重要的信息资源，在用户共享资源时可能会出现授权用户超出了他们的访问权限进行更改活动或非法用户绕过安全内核窃取信息资源等现象。因此，提出了数据库安全问题，也就是要保证数据的安全可靠和正确有效。对数据库数据的保护主要是针对数据的安全性、完整性和并发控制三方面。

数据的安全性就是保证数据库不被故意的破坏和非法的存取。数据的完整性是防止数据库中存在不符合语义的数据，以及防止由于错误信息的输入、输出而造成无效操作和错误结果。并发控制即数据库是一个共享资源，在多个用户程序并行地存取数据库时，就可能会产生多个用户程序并发地存取同一数据的情况，若不进行并发控制就会使取出和存入的数据不正确，破坏数据库的一致性。

所以在数据库设计时，必须考虑到这些问题。通常可采取一系列的安全策略和安全机制，其中主要是解决存取控制问题。可是对数据的存取控制并不足以对数据库用户进行约束，所以还要增加作业授权控制，把作业授权控制结合到安全策略中，并用自主型和强制性的存取控制来处理用户对数据的访问。而作业授权控制是处理用户对作业以及作业对数据的访问，这种作业授权控制既提供了高可靠性，又提供了应用的灵活性。

下面以著名的数据库Oracle和Fox或dBASE为例来说明。Oracle数据库系统是

一个非常有影响的分布式数据库系统，它不仅有国内广泛使用的微机版，而且还支持许多不同的操作系统。Oracle 数据库系统体系非常庞大，在此仅以 Oracle for NetWare 为例来说明其良好的自身保护机制。Oracle 是通过保护数据库的数据单元表（table）来保护信息资源不被其他程序进行非授权访问，从而达到保护自身的目的。Oracle 的表存储方式是由若干表组合在一起，以一个大文件的形式存放在 Novell 网络服务器的 Oracle 目录内的。这个文件的结构和加密方法对外均不公开，因而其他用户程序是无法破解这些表信息的，而且 Oracle 对外也不提供访问的接口。相比之下，Fox 或 dBASE 的自身保护机制就差得多，甚至可以说没有一点自身保护机制。众所周知，Fox 或 dBASE 的表存放在以 DBF 结尾的文件里，而结构完全是公开的。存放在 DBF 文件内的信息没有任何加密处理，非授权用户可以不通过 Fox 规定的方式访问 DBF 文件，因而很容易受到外来程序的攻击。这一点希望能引起所有基于 Fox 或 dBASE 建造的网络信息系统，尤其是金融、财务系统的管理人员的注意，对每天都要运行的系统的安全性给予高度重视。

#### 3. 其他威胁网络安全的典型因素

其他威胁网络安全的典型因素主要有以下几方面。

(1) 计算机黑客（将在后面的章节专门介绍）。

(2) 内部人员作案。有的员工可能会利用工作机会报复上司。此外如果系统管理员也成了黑客那麻烦就大了。

(3) 窃听。同轴电缆、双绞线、光纤或无线方式引入了新的物理安全暴露点，被动方式（如搭线窃听）或主动方式（如无线仿冒）。利用计算机通信设备天然存在的电磁泄漏进行窃取活动，也是一个重要的安全隐患。

(4) 部分对整体的安全威胁。任何一个单一组件的失密都可能造成整个网络的安全失败。

(5) 程序共享造成的冲突。共享同一程序可能会造成死锁、信息失效或文件不正确的开关状态。

(6) 对互联网而言可能有更多潜在的威胁，即使各网均能独立安全运行，联网之后也会发生互相侵害的后果。

(7) 计算机病毒。由于网络的设计目标是资源共享，所以网络是计算机病毒滋生和传播的理想家园。

### 1.2.4 缓冲区溢出

上网时间长的人都应该听说过缓冲区溢出，因为它的确是一个众人皆知、非常危险的漏洞，而且是个不分系统、程序都广泛存在的一个漏洞。以缓冲区溢出为类型的安全漏洞是最为常见，也是被黑客使用最多的攻击漏洞。所以了解缓冲区溢出方面的知识对于黑客、管理员或是一般的网民都是有必要的。

缓冲区（buffer）是用来存储程序代码和数据的临时区域，当程序或者进程试图向一个缓冲区内存入超过最初设定大小的数据时，就会发生缓冲区溢出（Buffer Overflow）。

缓冲区溢出期间到底会发生什么呢？缓冲区能够保存特定长度的数据，当向缓冲区

内存入超出其容量多得多的数据时，超出的部分必然会进入临近的缓冲区，覆盖其中保存的有效数据。

缓冲区溢出是非常普遍的一种安全漏洞，攻击者经常借此渗透远程网络，通过匿名方式获取对主机的访问或控制。此类攻击是 Internet 中最严重的一类安全威胁，因为其漏洞很普遍，而且利用起来很简单，是最常见的安全攻击，使攻击者有能力在远程系统中注入并执行代码，以取得特权访问。例如，OpenSSL 的远程缓冲区溢出形成的漏洞，会导致恶意用户获取系统的普通用户权限。

### 1. 缓冲区溢出机制

在程序试图将数据放到机器内存中的某一个位置的时候，因为没有足够的空间就会发生缓冲区溢出。人为的溢出是有一定企图的，攻击者写一个超过缓冲区长度的字符串，然后植入到缓冲区，向一个有限空间的缓冲区中植入超长的字符串可能会出现两个结果：一是过长的字符串覆盖了相邻的存储单元，引起程序运行失败，严重的可导致系统崩溃；另一个结果就是利用这种漏洞可以执行任意指令，甚至可以取得系统 root 特级权限。大多造成缓冲区溢出的原因是程序中没有仔细检查用户输入参数而造成的。

缓冲区是程序运行的时候机器内存中的一个连续块，它保存了给定类型的数据，随着动态分配变量会出现问题。大多时为了不占用太多的内存，一个有动态分配变量的程序在程序运行时才决定给它们分配多少内存。这样想下去，如果要给程序在动态分配缓冲区放入超长的数据，它就会溢出了。一个缓冲区溢出程序使用这个溢出的数据将汇编语言代码放到机器的内存里，通常是产生 root 权限的地方，这就不是什么好现象了。仅仅就单个的缓冲区溢出来看，并不是问题的根本所在。但如果溢出送到能够以 root 权限运行命令的区域，一旦运行这些命令，那就等于把机器的控制权拱手相让了。

缓冲区溢出漏洞有多种类型，但所有缓冲区溢出攻击的目标都是要接管对特权程序的控制，可能的话甚至是对主机的控制。为了达到目标，攻击者有两项任务，首先恶意代码要在程序代码地址空间内可用，其次特权程序应该跳转到代码的特定部分，确保合适的参数能够加载进入内存。

**注意**：*程序代码或者 shell 代码是在计算机操作员及操作系统之间提供接口的软件，换句话说，它是为用户提供内核接口的解释器。*

第一项任务可以通过两种途径完成，将代码注射到正确的地址空间或者利用现有的代码并对特定参数稍做修改。第二项任务有点复杂，因为要求修改程序的控制流，以使程序跳转到恶意代码。

### 2. 缓冲区溢出漏洞攻击方式

缓冲区溢出漏洞可以使任何一个有黑客技术的人取得机器的控制权甚至是最高权限。一般利用缓冲区溢出漏洞攻击 root 的程序，大都通过执行类似“exec(sh)”的执行代码来获得 root 的 shell。黑客要达到目的通常要完成两个任务，就是在程序的地址空间里安排适当的代码和通过适当的初始化寄存器和存储器，让程序跳转到安排好的地址空间执行。

1）在程序的地址空间里安排适当的代码

其实在程序的地址空间里安排适当的代码往往是相对简单的，但也同时要看运气如何。如果说要攻击的代码在所攻击程序中已经存在了，那么就简单的对代码传递一些参数，然后使程序跳转到目标中就可以了。攻击代码要求执行 exec('/bin/sh')，而在 libc 库中的代码执行 exec(arg)，当中的 arg 是个指向字符串的指针参数，只要把传入的参数指针修改指向/bin/sh，然后再跳转到 libc 库中的响应指令序列就可以了。当然了，很多时候这个可能性是很小的，那么就得用一种叫"植入法"的方式来完成。如果向要攻击的程序里输入一个字符串的话，程序就会把这个字符串放到缓冲区里，这个字符串包含的数据是可以在这个所攻击目标的硬件平台上运行的指令序列。缓冲区可以设在堆栈（自动变量）、堆（动态分配的）和静态数据区（初始化或者未初始化的数据）等的任何地方，也可以不必为达到这个目的而溢出任何缓冲区，只要找到足够的空间来放置这些攻击代码就够了。

2）将控制程序转移到攻击代码的形式

所有的这些方法都是在寻求改变程序的执行流程，使它跳转到攻击代码。最为基本的就是溢出一个没有检查或者其他漏洞的缓冲区，这样就会扰乱程序的正常执行次序。通过溢出某缓冲区，可以改写相近程序的空间而直接跳过系统对身份的验证。原则上来讲攻击时所针对的缓冲区溢出的程序空间可为任意空间，但因不同地方的定位相异，所以也就带出了多种转移方式。

（1）函数指针（function pointers）

在程序中，void( * foo)声明了一个返回值为 void 的函数指针的变量 foo。函数指针可以用来定位任意地址空间，攻击时只需要在任意空间里的函数指针邻近处找到一个能够溢出的缓冲区，然后用溢出来改变函数指针。当程序通过函数指针调用函数，程序的流程就会实现。这个可通过调用 Linux 下的 superprobe 程序体验一下。

（2）激活记录（activation records）

当一个函数调用发生时，堆栈中会留驻一个激活记录，它包含了函数结束时返回的地址。执行溢出这些自动变量，使这个返回的地址指向攻击代码，再通过改变程序的返回地址。当函数调用结束时，程序就会跳转到事先所设定的地址，而不是原来的地址。这样的溢出方式也是较常见的。如果使用漏洞扫描（UNIX 下的 SATAN 或者 NT 下的 Retina）器时，像多注意 stack smashing attack 的字样。

（3）长跳转缓冲区（longjmp buffers）

在 C 语言中包含了一个简单的检验/恢复系统，称为 setjmp/longjmp，意思是在检验点设定 setjmp(buffer)，用 longjmp(buffer)来恢复检验点。如果攻击时能够进入缓冲区的空间，感觉 longjmp(buffer)实际上是跳转到攻击的代码。像函数指针一样，长跳转缓冲区能够指向任何地方，所以找到一个可供溢出的缓冲区是最先应该做的事情。

3）植入综合代码和流程控制

常见的溢出缓冲区攻击类是在一个字符串里综合了代码植入和激活记录。攻击时定位在一个可供溢出的自动变量上，然后向程序传递一个很大的字符串，在引发缓冲区溢出改变激活记录的同时植入代码（C 语言在习惯上只为用户和参数开辟很小的缓冲

区）。植入代码和缓冲区溢出不一定要一次性完成，可以在一个缓冲区内放置代码（这个时候并不能溢出缓冲区），然后通过溢出另一个缓冲区来转移程序的指针。这样的方法一般用于可供溢出的缓冲区不能放入全部代码时使用。如果想使用已经驻留的代码不需要在外部植入的时候，通常必须先把代码做为参数。在 libc（熟悉 C 语言的朋友应该知道，现在几乎所有的 C 程序连接都是用它来连接的）中的一部分代码段会执行 exec（something），其中的 something 就是参数，使用缓冲区溢出改变程序的参数，然后利用另一个缓冲区溢出使程序指针指向 libc 中的特定的代码段。

对缓冲区溢出有兴趣的朋友，可以找到 eEye 公司开发的 Retina 发现 IIS 4.0 的那个缓冲区溢出漏洞引起的很多黑客攻击实例来看看。可以在 http://www.safefan.com（傲气雄鹰网络安全小组）找到关于它们的资料，做为网络管理人员最应该熟悉它们。

程序编写的错误造成网络的不安全性也应受到重视，因为它的不安全性已被缓冲区溢出表现的淋漓尽致了。

### 3. 缓冲区溢出保护

缓冲区溢出的漏洞被发现利用以来一直都是网络安全领域的最大隐患，很多安全人士均对这些漏洞做了仔细的研究，但是完全防止缓冲区溢出往往因为这样那样人为或其他的因素仍显得有点力不从心。下面就目前缓冲区溢出漏洞的几种保护方法做个简单的描述。

1）正确的编写代码

在编写代码的时候一般不会有人故意想要发生错误的，但是丝毫的错误往往会造成严重后果（C 语言编写的程序中字符串以“0”收尾，往往就是一个很不安全例子）。所以正确的编写代码是很关键的。

在编写时防止错误发生最原始的方法就是用 gerp 来找出源代码中较容易产生漏洞的库的调用。像对 sprintf 和 strcpy 的调用，这两个函数都不会检查参数输入的长度，有的在编写的时候采用了 sprintf 和 strcpy 的替代函数来防止，但是还是会有问题发生。因为这些错误的隐蔽性，所以就出现了查错工具 faultin-jection。faultin-jection 可以随时通过人为产生一些缓冲区溢出来找到代码的安全漏洞。只能说 faultin-jection 等类似的工具可以让编写时缓冲区溢出的漏洞更少一点，而完全没有则是不现实的。因为它们确实不可能找到所有的缓冲区溢出漏洞。编写时重复的检查代码漏洞可以使程序更加完美和安全。

2）非执行的缓冲区

在老版的 UNIX 系统中，程序的数据段地址空间是不可执行的，这样就使得黑客在利用缓冲区植入代码时不能执行。但是现在的 UNIX 和 Windows 系统考虑到性能和功能的速率和使用合理化，大多在数据段中动态形式的放入了可执行的代码，为了保证程序的兼容性，不可能使得所有程序的数据段不可执行。但可以只设定堆栈数据段不可执行，这样就很大程度上保证了程序的兼容性。UNIX、Linux、Windows、Solaris 都已经发布了这方面的补丁。

3）检查数组边界

数组边界检查完全没有缓冲区溢出的产生，所以只要保证数组不溢出，那么缓冲区溢出攻击就只能是望梅止渴了。进行数组边界检查时，所有对数组的读写操作都应该被检查，这样可以保证对数组的操作在正确的范围之内。检查数组是一件烦琐的事情，所以利用一些优化技术来检查可减少负重。可以使用 Compaq 公司专门为 Alpha CPU 开发的 Compaq C 编译器、Jones&Kelly 的 C 的数组边界检查、Purify 存储器存取检查等来进行。

所有缓冲区溢出漏洞都归于 C 语言的“功劳”。只有类型安全的操作才可以被允许执行，这样就不会出现对变量的强制操作。Java 和 ML 等被认定为类型安全的语言，但作为 Java 执行平台的 Java 虚拟机是 C 程序，所以攻击 JVM 的途径就是使 JVM 的缓冲区溢出。完整性检查在性能上有着很大的优势，并且有良好的兼容性。

对付缓冲区溢出攻击的方法有多种，最重要的是小心编写正确的代码。软件开发团队必须知道如何编写安全的程序。程序员可以借助工具和技术来编写对缓冲区溢出攻击具有免疫力的代码段。

另一种方法是让程序代码的数据缓冲区（内存位置）地址空间不可执行，此类地址空间禁止执行代码。攻击期间，程序的缓冲区可能已被渗透进入。就像前面讲的，努力将代码注射到程序空间中只是缓冲区溢出攻击的一个条件，另一个关键的条件是接管程序的流控。如果在程序开发的调试阶段实施了数组边界控制或者数组边界检查，此类威胁就可以被消除。这种检查能够确保缓冲区保持在正确的预定义范围内，也能核实缓冲区根本不可能溢出。

**4. 对策**

本章到这里只是介绍了缓冲区溢出漏洞、攻击和一些防范方法，理解缓冲区溢出机制是很重要的，因为它们是所有目前网络互联基础设施面临的远程渗透问题的根源。接下来的章节中将会探讨这些远程渗透漏洞问题，并且讨论更多的防御和保护方法（访问过滤器、入侵检测系统和审计工具）。

## 1.2.5 欺骗技术

一般来说，攻击者可以利用欺骗方法来危害计算机系统。很多人误以为欺骗是一种实际的攻击，事实上欺骗只是攻击者在试图利用两台主机间关系过程中的一个步骤。这里要讨论的有 3 种欺骗技术（其中而有关 IP 地址欺骗还将在第 2 章中详细讨论）。

**1. IP 地址欺骗（IP spoofing）**

在很多攻击类型中，攻击者都会用另一个地址来替换发送者的 IP 地址，或者比较少见的会更改目的地址。IP 欺骗（IP spoofing）通常被用来突破一个目标主机。此外，IP 欺骗也被用作发起拒绝服务（denial-of-service，DoS）攻击。如图 1-2 所示，在一次 DoS 攻击中，攻击者修改 IP 分组，误导目标主机，使其以可信任主机方式接受最初的分组。攻击者必须知道被信任主机的 IP 地址，并且修改分组头部（源 IP 地址），以便让其看起来像是

被信任的主机。

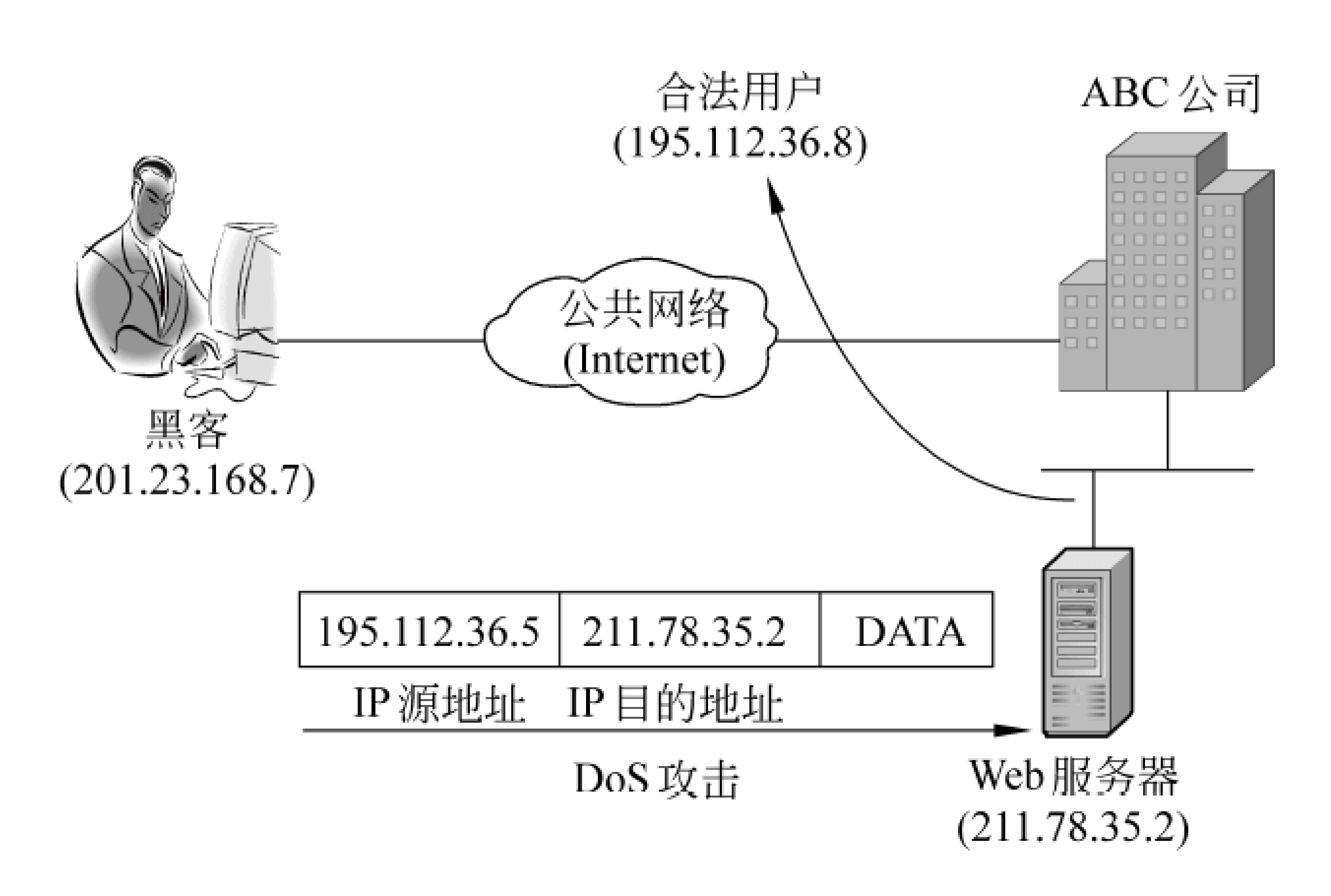



**图 1-2　利用 IP 欺骗进行 DoS 攻击**

### 2. ARP 欺骗

地址解析协议(address resolution protocol,ARP)提供了将已知 IP 地址解析或映射成 MAC 子层地址的机制。图 1-3 中,两台主机试图通过像以太网这样的多访问介质开始一次对话。

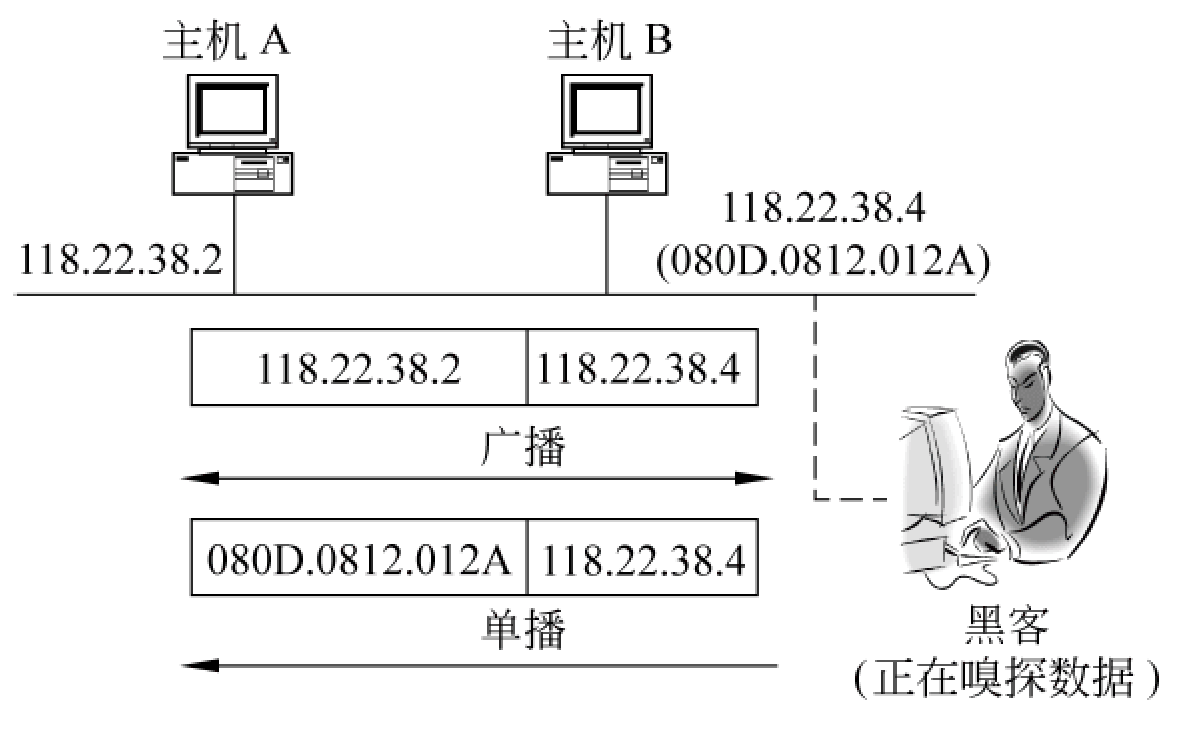



**图 1-3　ARP 欺骗**

主机 A 想要发起和主机 B 的会话,但是需要 IP 地址和 MAC 地址。在会话建立期间,主机 A 只知道主机 B 的 IP 地址 118.22.38.4。为了确定数据报的目的 MAC 地址,主机 A 自先检查本地的 ARP 缓存表,如果 MAC 地址不在此列,主机 A 就会发送一个 ARP 请求,这是一个企图寻找带有 IP 地址 118.22.38.4 的目的主机的广播分组。每一个网络中的主机都能收到。这里没有真正的认证,两台主机间的校验仅仅基于硬件地址,这是 ARP 过程的薄弱环节。借助 ARP 欺骗,攻击者就能够利用这种硬件地址认证机制,假冒主机 B 的硬件地址。一般来说,攻击者能够欺骗本地网络中的任何主机或网络设备,使这些设备相信攻击者的工作站就是可信的主机。这种攻击手段常见于交换式环境中。

**3. DNS 欺骗**

域名服务(domain name service,DNS)可以让网络客户端基于远程系统的名字来获取其 IP 地址。主机向 DNS 服务器发送包含远程系统名字的请求,DNS 服务器以相应的 IP 地址做出响应。DNS 欺骗是这样一种手段:黑客努力使目标主机相信,其所要连接的正是攻击者的主机。攻击者修改了一些记录,使主机的名字条目对应到攻击者的 IP 地址,这种情况下整个 DNS 服务器都被攻击所占据。

**4. 对策**

要防止 ARP 欺骗,可以在网络中所有的主机和路由器上实施静态 ARP 表。当然,也可以用一台 ARP 服务器来代表目标主机对 ARP 请求做出响应。为了对付 DNS 欺骗,可以用反向查询来检测攻击,反向查询是一种以名字来校验 IP 地址的机制。IP 地址和名字文件通常保持在不同的服务器上,这可以让破坏活动更难实施。到现在,只是讨论两种欺骗手段以及相关对策,更多预防和保护方法(访问过滤器、入侵检测系统和审计工具)可在后续章节中看到。

# 1.3 网络安全发展趋势展望

## 1.3.1 网络安全的现状

**1. 近几年网络安全回顾**

随着网络的技术不断发展、进步,网络安全面临的挑战也在增大。一方面,对网络的攻击方式层出不穷。随着硬件技术和并行技术的发展,计算机的计算能力迅速提高,原来认为安全的加密方式有可能失效。1996 年报道的攻击方式有 400 种,1997 年达到 1000 种,1998 年达到 4000 种,两年间增加了十倍。攻击方式的增加意味着对网络威胁的增大。随着解密理论、硬件技术和并行技术的发展,计算机的计算能力迅速提高。原来认为安全的加密方式有可能失效,如 1994 年 4 月 26 日人们用计算机破译了 RSA 发明人 17 年前提出的数学难题“一个 129 位数字中包含的一条密语”,而在问题提出时预测该问题用计算机需要 850 万年才能分解成功。针对安全通信措施的攻击也不断取得进展,如 1990 年 6 月 20 日美国科学家找到了 155 位大数因子的分解方法,使“美国的加密体制受到威胁”。近年来我国科学家在破解 HASH 函数方面取得了长足进步,成功破解了著名的 MD5 和其他几个 HASH 函数。

另一方面网络应用范围的不断扩大,特别是人类社会生活对 Internet 需求的日益增长,使人们对网络依赖的程度增大,网络安全逐渐成 Internet 及各项网络服务和应用进一步发展的关键问题。1993 年以后 Internet 开始商用化,通过 Internet 进行的各种电子商务业务日益增多,加之 Internet/Intranet 技术日趋成熟,很多组织和企业都建立了自己的内部网络并与 Internet 连通。上述电子商务应用和企业网络中的商业秘密均成为攻

击者攻击的目标。据统计,目前网络攻击手段有数千种之多,使网络安全问题变得极其严峻。据美国商业杂志《信息周刊》公布的一项调查报告称黑客攻击和病毒等安全问题在2000年造成了上万亿美元的经济损失,在全球范围内每数秒钟就发生一起网络攻击事件。

从网络安全威胁的发展趋势上看,系统漏洞问题、混合了黑客攻击和病毒特征于一体的网络攻击和以窃取用户机密数据为目的的威胁,将成为近几年网络安全威胁的主要形式。除了微软的漏洞外,目前像思科路由器、Oracle数据库、Linux操作系统、移动通信系统以及很多特定的应用系统中,均存在着大量的漏洞。系统漏洞从出现到被利用之间的时间将会越来越短,直至零时间。2003年8月份出现的"冲击波"病毒利用的是仅公布了26天的漏洞。控制系统中的漏洞已成为人们必须要考虑的首要问题。目前的病毒早已不再是传统的病毒了,而是集黑客攻击和病毒特征于一体的网络攻击行为。针对这种混合性的威胁仅仅靠反病毒产品是无法对付的,必须增加防火墙、IDS以及反病毒等综合防范措施。此外,虽然近来的一些恶意代码只是阻塞网络,引起网络速度的极端下降,但是一些以窃取用户机密数据的威胁开始在网上流行,如网络钓鱼(Phishing,是Fishing和Phone的综合体。由于黑客始祖起初是以电话作案,所以用Ph来取代F,创造了Phishing)。钓鱼式攻击利用欺骗性的电子邮件和伪造的Web站点来进行诈骗活动,企图通过电子邮件或即时通信信息,把用户诱骗至有官方外观的假冒网站,冒充真正需要信息的人,欺诈性地获取敏感的个人信息(比如密码和信用卡细节)的行为,是社会工程攻击的一种形式。受骗者往往会泄露自己的财务数据,如信用卡号、账户用户名、密码和社保编号等内容。诈骗者通常会将自己伪装成知名银行、在线零售商和信用卡公司等可信品牌,在所有接触诈骗信息的用户中,有高达5%的人都会对这些骗局做出响应。早期的案例主要在美国发生,但随着亚洲地区的Internet服务日渐普遍,有关攻击也开始在亚洲各地出现。从外观看,与真正的银行网站无异,却在用户以为是真正的银行网站而使用网络银行等服务时将用户的账号及密码窃取,从而使用户蒙受损失。防止在这类网站受害的最好办法就是记住正宗网站的网址,并当链接到一个银行网站时,对网址进行仔细对比。在2003年,香港地区也有多起此类案例出现,有网站假冒尚未开通网上银行服务的银行,利用虚假的网站引诱客户在网上进行转账,但其实把资金转到网站开设者的账户内。而从2004年开始,有关诈骗也开始在中国内地出现,曾出现过多个假冒的银行网站,比如假冒的中国工商银行网站。

### 2. 网络安全新趋势

目前,攻击方式主要是利用各种恶意插件控制用户的计算机,支持Storm网络的更新和发展。此外,使用受感染的系统托管特定的登录页,这些登录页与垃圾邮件、网络钓鱼和信息欺诈中包含的内容直接相关。从2007年11月份开始,网络系统攻击渐渐成为了主流。在2007年,网络安全威胁出现了两个新的现象:一是具有"链接型"特征的混合攻击出现;二是平台化攻击。大量的经验表明,当前安全威胁的主要趋势是复杂度提高。大量的黑客采用垃圾邮件、恶意软件和数据窃贼等传统的攻击手段。但是,这些攻击却变得更加复杂,而且得到不断改进。

回顾2007年的重大事件就可以发现,以Flux(钓鱼、恶意软件隐藏技术)、分布式命令和控制(DC)、循环利用包(REP)为代表的攻击技术不断出现。此前趋势科技的安全专家表示,当前很多专业攻击者甚至开始创建后端恶意软件管理系统,以维持感染机器的数量并及时监控插件的利用效果。从去年开始,具有"链接型"特征的混合威胁攻击不断出现,通过利用垃圾邮件,其内建的链接指向攻击者网站或者钓鱼站点,意在感染用户的计算机或者直接进行欺诈。新型的混合威胁利用垃圾邮件作为传播的源头,整合了钓鱼和恶意欺诈的攻击形式,在攻击的同时还在被攻击的计算机中种植僵尸程序,并借助邮件和僵尸网络一起扩大影响。

利用垃圾邮件作为攻击源头,同时整合僵尸网络技术进行多渠道扩散,已经成为当前混合威胁的新形式。由于此类攻击的整合性可以将钓鱼、恶意插件等多种供给手段组合于其中,因此威胁相当可观。目前在此领域以Feebs和Clagger攻击最有代表性。此外,为了便于进行网络钓鱼,通过URL而不是传统的邮件扩散的Feebs攻击的爆发次数也大大增多。根据IDC的统计,利用URL开展网络钓鱼的恶意攻击平均每年增加253%,并表现出了多阶段攻击发展中的分布趋势,这些攻击尝试以多种方式发送看起来无害(如纯链接的电子邮件)的信息,但是当其中的URL指向一个被恶意软件感染的Web服务器时,会导致严重的安全风险。

如果说Feebs和Clagger开启了多渠道攻击的大门,那么Storm的出现则将平台化攻击引入现实。Storm系列恶意软件联合新开发的和现有的恶意软件技术,创建了一个高度复杂的攻击平台。Storm将不同的技术整合成一个更大的系统,无论是在源头还是规模方面,这个系统都更难于追踪,其行动快速、动力十足。作为混合性威胁,它使用电子邮件和Web进行双重攻击。事实上,Storm威胁的精髓在于整合后的"饱和攻击",在安全业界Storm经常被称做Storm木马、Storm僵尸网络、Storm蠕虫、Storm垃圾邮件引擎、Storm分布式拒绝服务网络。这说明了Storm具有各种特征,也说明它是一种新型的恶意软件,一种可重复再生的恶意软件。这种威胁将钓鱼、欺诈、恶意软件、木马、入侵等多种手段集于一身,防不胜防。

目前来看,能够称为"平台化袭击"的技术前提至少有六个。

(1) 能够实现自我繁殖。Storm以发送海量垃圾邮件方式进行扩散。用户被指向多个不断变化的URL,这些URL为Storm恶意软件服务。系统如果被感染,就会成为Storm网络的一部分。

(2) 对等性。以前的僵尸网络是通过一个分等级的管理结构被集中控制,而Storm节点通过独特的对等通信协议互相联络,所以要追踪其总规模十分困难。

(3) 协作特性。Storm发送指向其他Storm计算机托管的网页的垃圾邮件,其网络发起攻击的方式异常复杂。

(4) 可重用性。以前的恶意软件攻击是神风突击队式的。一旦发动,就会一直运行,直至油尽机毁,最终在互联网中消失。而Storm不是一次性的恶意软件,它是一个可以改变、延伸和重用的平台。这种适应性使得它在2007年生存发展下来,并迈进2008年。

(5) 集成性。Storm可用来发动多种攻击,如垃圾邮件、网络钓鱼和DDoS等。它还因危害IM网络和张贴垃圾博客信息而成为多种网络协议的主要威胁。

(6) 自我防御。作为平台化袭击的核心,Storm 能够监控逆向工程或分析迹象,针对研究者和反垃圾邮件组织反复发动拒绝服务攻击。

根据目前披露的信息可以发现,Storm 集电子邮件和 Web 攻击于一身,形成一个双重攻击系统,随之形成了一种有趣的同步现象:Storm 僵尸网络发送垃圾邮件,其他僵尸网络专注于恶意网页。这样一来,就大大提高了网络钓鱼和交易欺诈的效率。

此外,为了使 Storm 病毒的危害更大,很多专业黑客在其中加入了 Drive-by 浏览器劫持程序,无须下载任何可执行文件,仅仅通过浏览网页就能够感染易受攻击和未打补丁的计算机。

一旦用户中招,被 Storm 感染的系统将连接成一个对等的 P2P 网络,以保持冗余和分布式通信。在 Storm 出现之前,僵尸网络依靠集中指挥和控制的结构,它们经常使用 IRC 通道,等待操纵者的指令。但是,这种设计有一个弱点,通过关闭中央 IRC 通道或阻截对其的访问,就能有效地使僵尸网络"身首异处",使之成为一堆废物。Storm 吸取了这些弱点的教训,转而采用分布式指挥和控制结构。

为了保持生命力和预防逆向工程,Storm 具备了自我防御特性。如果对它的检查太接近,它会自动地发动分布式拒绝服务攻击。在此情况下,当一个新的系统加入 Storm 网络,它会被用来执行各种类型的攻击,包括发送 Storm 吸收垃圾邮件以发展 Storm 网络;为网络钓鱼和恶意网页服务;攻击即时通信客户;提供 Fast-fulx 和 DNS 解决方案;在网站上张贴垃圾博客信息。另外,Storm 僵尸网络能够根据需要改变用途,进行循环攻击。整个网络能够保持同步和协作,以确保垃圾邮件与基于 Web 的登录页面的联系。

## 1.3.2 网络安全技术的发展

网络安全经过了 20 多年的发展,已经发展成为一个跨多门学科的综合性科学,它包括了通信技术、网络技术、计算机硬件设计技术、计算机软件技术、密码学、网络与计算机安全技术等。

从理论上分析,网络安全是建立在密码学和网络安全协议的基础上的。密码学是网络安全的核心,利用密码技术可以对信息进行加密传输、加密存储、数据完整性鉴别、用户身份鉴别等。它比传统意义上简单的存取控制授权等技术更可靠。加密算法是一个公式和法则,它规定了明文和密文之间的变换方法。由于加密算法的公开化和解密技术的发展,再加上发达国家对关键加密算法的出口限制,各个国家正不断致力于开发和设计新的加密算法和加密机制。对于安全协议方面,众多标准化组织制定了许多标准和草案,尤其是以 RFC 文稿出现的协议标准更是成了网络安全设备的基础,例如,虚拟专用网(virtual private network,VPN)技术就是建立在安全隧道基础上的,点对点的隧道协议(PPTP:RFC2637)和第 2 层隧道协议(L2TP:RFC2661)提供了远程 PPP 客户到 LAN 的安全隧道。因此,网络安全的实现需要不断发展和开发满足新的需求的安全协议。

从技术上分析,网络安全取决于两个方面:网络设备的硬件技术和软件技术。网络安全是由网络设备的软件和硬件互相配合来实现的。但是,由于网络安全作为网络对其信息提供的一种增值服务,往往会发现安全软件的处理速度成为网络系统的"瓶颈"。因

此,将网络安全的密码算法和安全协议用硬件实现,实现线速的安全处理仍然将是网络安全发展的一个主要方向。

因此,在安全技术不断发展的同时,全面加强安全技术的应用也是网络安全发展的一个重要内容。因为即使有了网络安全的理论基础,没有对网络安全的深刻认识和广泛地将它应用于网络中,那么谈再多的网络安全也是无用的。例如,系统的安全构架建立、安全设备的应用、安全制度与安全培训、各种恶意代码的防范、服务器数据的安全备份等应用。同时,网络安全不是病毒防治、入侵检测、防火墙、身份认证、加密等产品的简单堆砌,而是包括从系统到应用、从设备到服务的完整的、体系性的安全系列产品的有机结合。

对于我国而言,网络安全的发展趋势将是逐步具备自主研制网络设备的能力,自发研制关键芯片,采用自己的操作系统和数据库以及使用国产的网络管理软件。中国计算机安全的关键是要有自主的知识产权和关键技术,从根本上摆脱对外国技术的依赖。

通过以上内容可以看出,网络安全是个系统工程。只有当网络中每个用户都具备了网络安全防范意识,并且实现了安全服务与机制、安全应用与管理的全面结合,才能构建一个具有整体防御能力的安全网络系统。

### 1.3.3 建立主动防御体系

从网络诞生的那一天开始,应用与安全之间的博弈就一直未曾停止。病毒和蠕虫让终端 PC 无法正常高效运行,后门程序和木马让企业保密信息时刻经受被泄露的危险,DoS/DDoS 攻击和黑客的恶意破坏不时让企业的网络面临瘫痪边缘,更不用说更多由于应用和管理不完善为业务网络带来的种种问题。于是防火墙、防毒墙、入侵检测、入侵防护防病毒软件等越来越多的安全产品部署在了网络之中,但是在各种安全威胁的面前,网络却始终处于被动。难道在网络安全威胁面前就束手无策了么?当然不是。我们所欠缺的是对安全防护的综合匹配,将安全防护深度融合到业务网络之中,并由被动防护转变为主动防御,才能在日渐繁复的网络环境中应对自如。

**1. 主动防御,应对下一代安全隐患**

进入新世纪以来,随着各种企业业务对网络的依赖性日益增加,基于网络平台的 DoS 攻击由蠕虫、病毒木马程序相结合的混合攻击以及广泛出现的系统漏洞攻击、黑客攻击和 Turbo 蠕虫等安全威胁也日益泛滥,且传播速度也加快到以分钟计,原有的以人工防御为主的安全措施则逐步淘汰,取而代之的是以硬件防护产品为主的自动响应防护工具。然而虽然自动响应的安全防护措施能够基本满足当前的网络安全需求,但不难看到在近年来日趋频繁的针对基础设施漏洞的破坏性攻击、由大规模蠕虫和 DDoS 攻击导致的瞬间网络威胁以及破坏有效负载的病毒和蠕虫,将成为下一代网络威胁的主体。安全威胁的传播速度也将提升到以秒计,对当前安全设备的自动响应能力将提出全新的挑战,正是在这样的趋势引导下为应对即将到来的下一代网络安全隐患,有必要提前进行部署,将业务网络的安全防护由现在的自动响应升级为主动防御和阻挡,只有如此网络安全防护才能在未来与安全威胁的时间赛跑中占据领先的地位。

### 2. 深度渗透打造综合防御

目前企业所面临的安全问题越来越复杂，安全威胁正在飞速增长，尤其混合威胁的风险（如蠕虫、DDoS 攻击、垃圾邮件等）极大地困扰着用户，给企业的网络造成严重的破坏。那么如何才能实现企业业务网络的最有效防护呢？显然，首先需要打破传统的希望安全防护产品“一夫当关、万夫莫开”的理想化期待，未来的网络安全防护必然是深度融合在各个业务网络模块内协同工作的综合防御体系。一些业内专家指出经过数年的技术发展，基于专业 ASIC 芯片和 NP 技术的硬件防火墙虽然防护能力和过滤性能均有了大幅度的提升，但仅仅依靠防火墙来实现全网安全是不可行的。目前造成网络威胁的诱因有很多不能够为防火墙所识别。一方面，随着企业内部网络越来越庞大和复杂，越来越多的网络威胁可能来自于企业内部，包括病毒的传播、非法流量甚至于恶意破坏都可能是在“门”里面进行的。那么“门”的隔离效果显然不能实现，而这些威胁足以让企业的网络面临瘫痪。另一方面，防火墙基本都是针对网络结构的 L3—L4 层的安全防护，而现在越来越多的威胁均来自于应用层，即网络结构的 L7 层，相当于更多的安全威胁都会“调整体形”，然后以“门”所能接受的规格和尺寸顺利进入企业网络。由此可见防火墙固然必不可少，但是却远远不够。据相关数据统计，如果单独依靠防火墙仅能够抵御约 20％左右的安全威胁。因此，需要对安全威胁进行更深层次的防护才能够确保安全。目前业内比较常见的包括 IDS（入侵检测系统）和 IPS（入侵防护系统）两种都是针对应用层威胁所采取的安全措施。IDS 相当于在室内安装了可以监视所有人员、物品的“摄像头”，一旦有安全隐患在室内发生，摄像头就会第一时间进行系统报警让管理人员进行及时处理。然而网络威胁的传播速度正在以分秒为单位快速蔓延，IDS 尽管能够在第一时间发现问题却无法直接处理这个时间差，往往造成企业的大量损失。IPS 的出现则恰恰弥补了 IDS 的不足，它就像一道“纱窗”安装在防火墙开辟的“窗口”上，有效地对出入企业的数据进行深层次的检测，并把非法流量和安全隐患在第一时间“拒之门外”。然而，面对越来越复杂的网络应用环境，要真正实现端到端的网络安全，只有将安全防护全面渗透进网络应用的各个环节，使之成为一张安全的网络，才能在未来安全与威胁的博弈中占得先机。不难看出主动防御和深度渗透的综合安全防护网络的时代正在迎面走来。

### 3. 进入全面防御时代

综上所述，当前的安全危机与形式的复杂度均超过了以往，用户的安全威胁是全方位的，传统上仅仅依靠简单产品就能确保安全的时代已经过去了，面对复杂的垃圾邮件、网络钓鱼和恶意欺诈，有效的应对之道将是全面防御，从网络和应用的各个层次入手，保持安全的上下可控。

举例来看，以往很多安全厂商提出了用传统型 URL 过滤器对网站进行分类，以拦截危险的网站或行为。但是，当受信网站被黑并携带恶意代码时，这样做便无法提供有效的保护。对于企业来说，这种技术上的变化使得员工即使进行“安全浏览”，避免接触有问题的网站，也会带来风险。再比如许多 Mpack 攻击采用恶意软件来感染系统，试图从受感染的系统盗窃数据，并将其发送回大本营。但目前许多企业配置的防火墙设计无法

监控或拦截从公司网络内部发起的数据传输，特别是当这些传输以正常的用户活动为基础的时候。另外，即使企业采取对进入的电子邮件流进行病毒扫描，以及使台式机的防病毒软件保持更新等措施，也同样无法满足要求。因为 Mpack 利用被认为是安全网站的 HTTP，并不涉及电子邮件渠道。

对此当前很多新型攻击的多阶段、多协议特性使得以前的一些最佳安全实践变得过时。一流的防垃圾邮件网关在多样性和数量方面，也无法跟上垃圾邮件的发展速度。在保护用户免遭许多通过 HTTP 发出的新型攻击方面，传统的 Web 代理设备（充当缓存并强制执行 Web 浏览安全策略）已经无法满足要求。

因此，当前业界一致认为，如果要在这种混合攻击的前提下防御网络钓鱼、垃圾邮件，以及恶意软件欺诈等威胁，用户就必须从以下四点考虑安全建设的蓝图。

1）保护 Web 数据流的安全

无疑，Web 环节已经成为企业威胁的入口，在此领域部署全面的 Web 安全网关（包括 HTTP 过滤网关）将是不可忽视的一环。需要注意的是，Web 安全网关并非传统的 URL 过滤。事实上，即使企业用户部署了 URL 过滤方案来对个人 Web 使用行为进行控制和报告，这些数据库也不足以避免恶意软件下载到企业的网络之中。URL 过滤器的安全分类保护在一个阶段内是静态的，无法提供全程实时的 Web 对象扫描。经验证明，依靠安全清单防御恶意软件，类似于使用静态的黑名单来防御垃圾邮件，效果非常有限。恶意软件分发者将其恶意代码插入遭到入侵的“合法”网站的技术越进步，URL 过滤保护就越无用。

2）部署对电子邮件的预防性保护措施

随着一系列新型恶意木马、病毒的发展，“传统的”病毒分发途径（电子邮件）依旧需要先进的保护措施。对用户来说，可扩展的多核心垃圾防护设备是未来的发展方向。另外，一些安全厂商开始采用 IP 声誉系统来过滤垃圾邮件站点，这样在连接层拦截输入的攻击，降低了防垃圾邮件网关和网络总体数据流通的负担。

3）预防企业数据丢失

此前深信服的安全专家邬迪在接受采访时表示，很多木马程序旨在扫描用户的硬盘，将重要信息（账号、密码等）发送回指挥控制中心。但是，没有感染木马也有可能丢失数据，其中主要是由于企业的员工失误造成的。因此他的看法是，防范外部威胁进入网络盗取重要信息至关重要。与此同时，针对可能的违反政策行为对输出的通信进行扫描或者延时审计也非常有必要。

4）跟踪重要通信

对于企业防御系统来说，有一个事实必须认识到，当前以垃圾邮件为载体的钓鱼和欺诈攻击数量在翻番增长。在这种情况下，企业需要对邮件系统进行控制与追踪。据了解，目前国内已经出现了可对电子邮件信息进行实时追踪的新技术，这种技术与物理包裹投递时所使用的技术类似。有安全专家表示，这种技术将为企业的法规遵从性建设提供帮助。

# 习　题　1

## 1. 填空题

(1) 一般情况下机密性机构的可见性要比公益性机构的可见性________(填高或低)。

(2) 计算机网络安全受到的威胁主要有:________和________。

(3) 对数据库构成的威胁主要有:篡改、损坏和________。

(4) UNIX 和 Windows 2000/2003 操作系统能够达到安全级别是________。

(5) 网络系统的________是指保证网络系统不因各种因素的影响而中断正常工作。

## 2. 问答题

(1) 什么是网络安全?

(2) 目前网络安全的主要威胁及隐患有哪些方面?

(3) 如何理解网络安全的基本需求和管理策略?

(4) 网络安全与单机系统的安全有何区别?

(5) 网络安全的安全级别是如何分类的?

(6) 对网络进行安全管理需要哪些措施?

(7) 网络安全有哪些新的趋势?

(8) 针对网络安全新的动态,如何构建防御体系?

# 第 2 章 chapter 2

# 网络安全体系

处于不同的角度，对网络安全有着不同的认识。许多人喜欢从一个具体的实物，如防火墙、入侵检测、VPN 等来看待网络安全，这是很不全面的。尽管这些产品与技术在网络安全中扮演了重要角色，但是网络安全更为复杂，它不是一个产品的迭加。网络安全是一个系统，所有的网络安全起始于安全策略，它将范围扩展到负责遵循该策略以及必须加强它的人们。如果不从体系结构角度来考虑网络系统的安全性，忽略建立安全标准体系，往往会造成网络整体功能不完备、存在薄弱环节、部件功能重复、效率低下、评估困难、不适应需求和技术变化、相互操作困难等问题。因此，建立网络安全体系的目的是从管理和技术上保证安全策略得以完整准确的实现，安全需求得以全面准确地满足。具体则包括确定必需的安全服务、安全机制和技术管理以及它们在系统上的合理部署和相关配置。

## 21 网络安全体系层次

作为全方位的、整体的网络安全体系应该是具有层次性结构的，不同层次反映了不同的安全问题，并根据不同的安全问题采取相应的安全措施。一般情况下，根据网络的应用情况及其结构特点，可以将网络安全体系依次划分为物理层安全、系统层安全、网络层安全、应用层安全和管理层安全。

### 21.1 物理层安全

物理层安全是整个计算机网络系统安全的前提。它涉及多方面的内容，主要是用来保证各种计算机网络系统设备设施等免遭地震、水灾、火灾等环境事故以及人为操作失误或其他错误而导致的破坏过程，还包括对网络设备的环境、软硬件的安全控制。一般情况下，可以通过采用各种技术手段，来保证设备的运行温度、湿度、烟尘和电力系统以及通信线路的畅通。如通过采用高可用性的硬件和充足的设备备件及采以可拆卸设备来提高设备的备份能力，采用电视监控等技术与手段来提高设备的防盗、防毁、防电磁信息辐射泄露、防止线路截获、抗电磁干扰等能力。通过这些技术与方法的综合应用来对网络系统所在的物理层进行全方位的安全保护。

### 2.1.2 系统层安全

系统层的安全问题主要来自网络内使用的操作系统的安全，主要表现在三方面：一是操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制、系统漏洞等；二是对操作系统的安全配置问题，由于配置不当而引起的安全事故也是常见的问题；三是各种病毒对操作系统的威胁。对于系统层的安全防范可以选用安全性高的操作系统，并对系统进行周密的安全配置提高操作系统的安全性，通过专业的安全工具（安全检测系统）定期对其进行安全评估，及时升级系统、修补系统漏洞。由于操作系统是其他应用软件的基础平台，如果不能采用有效措施来保障系统层的安全性，则无论在应用层上采取任何措施，系统的安全都无法得到有效保证，对于操作系统的安全在相关章节会做详细介绍。

### 2.1.3 网络层安全

网络层安全问题主要体现在网络协议方面的安全性，包括网络层身份认证、网络资源的访问控制、数据传输的保密性与完整性、路由系统的安全、入侵检测的手段以及网络设施防病毒等。在这个层面上，网络通信的授权、传输的加密和审计记录以及加强登录过程的认证，确保用户的合法性是重点考虑的内容。技术方法上除了采用访问控制和系统漏洞检测外，还可以采用访问存取控制，对权限进行分割和管理。目前网络广泛采用TCP/IP 协议，由于协议自身存在的一些问题，导致在网络层上的安全内容最为复杂，也是本书重点探讨的内容。

### 2.1.4 应用层安全

应用层安全问题主要由提供具体应用服务所引发的，主要是指应用软件及数据的安全性，既包括在网络上常用的 WWW 服务、电子邮件系统、DNS 系统等，也包括大量的基于网络的其他应用系统，如数据库、信息管理系统等。在开发应用具体的应用系统时，如果不注意开发规范，或没有对代码进行严格测试，应用系统的安全是相当薄弱的。这就要求应用系统的开发一定要采用规范化的开发过程，尽可能减少由于程序设计不当而带来的安全漏洞。

### 2.1.5 管理层安全

管理层安全主要包括安全管理制度、部门与人员的组织规则等。构建一个完备的网络安全系统并不完全取决于技术手段，离开了科学管理，安全便无从谈起。科学完善的管理是网络安全真正得以实施的保证。管理的水平在很大程度上影响着整个网络的安全水平。严格的安全管理制度、明确的部门安全职责划分、合理的人员配置都可以在很大程度上降低其他层次的安全漏洞。所以在各项安全技术得到保证的情况下，必须建立严密的计算机管理规章制度和运行规程，并建立良好的故障处理反应机制，来保障网络系统的安全正常运行。

# 2.2 OSI/ISO 7498-2网络安全体系结构

随着互联网应用的快速发展,网络安全已深入到诸多领域,人们对于网络安全的认识也是一个由浅入深的过程。当各种安全威胁来临之时,如何在日益增长并更为复杂的各种应用中有效地进行自我保护,建立科学的网络安全体系,对于指导我们全面科学地构建网络安全极为重要。传统上的方法与过程是对网络进行风险分析,制定相应的安全策略,采取一种或多种安全技术作为防护措施。这种安全分析方法在很大程度上针对固定的威胁和环境弱点。对于网络的特点而言,安全是一个动态的、不断完善的过程。在建立网络安全模型的过程中,人们进行了大量的探索,网络安全模型也经历了由静态到动态、由局部到整体、由平面到立体的发展过程。

## 2.2.1 安全体系结构模型的发展

### 1. PDR安全模型

最早提出来的安全模型称为PDR模型。PDR是防护(protection)、检测(detection)、反应(reaction)的缩写,其基本的原理就是信息安全的所有活动,不管是攻击行为、防护行为、检测行为还是响应行为等都需要消耗时间。安全离开时间是没有意义的,因此可以用时间来衡量一个体系的安全性和安全能力。

### 2. P2DR安全模型

P2DR安全模型是可适应网络安全理论的模型,在整体的安全策略的控制和指导下,在综合运用防护工具的同时,利用检测工具来了解和评估系统的安全状态。P2DR模型包括4个主要部分,分别是策略(policy)、防护(protection)、检测(detection)和响应(response)。它们构成了一个完整的、动态的安全循环,在安全策略的指导下保证信息系统的安全。P2DR安全模型认为一个良好的完整的动态安全体系,不仅需要利用操作系统访问控制、防火墙、加密等恰当的防护,还需要加入动态的检测机制,如入侵检测,漏洞扫描等。在发现问题时还需要及时做出响应。这样的一个体系需要在统一的、一致的安全策略的指导下实施,由此形成一个完备的闭环的动态自适应安全体系,如图2-1所示。

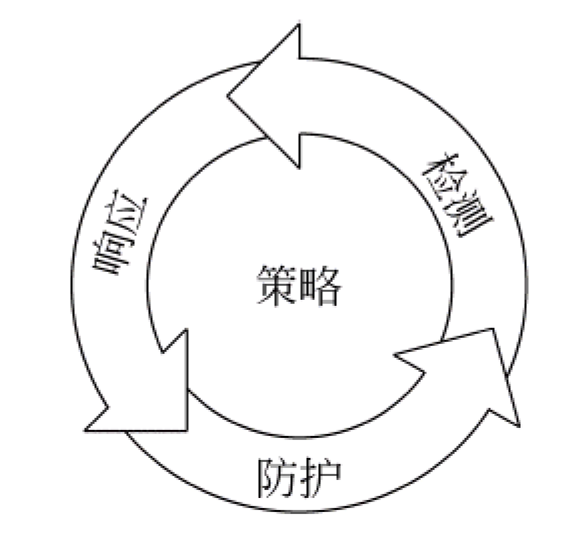



**图2-1 P2DR安全模型**

### 3. PDRR安全模型

PDRR模型是在经典的P2DR模型基础上演变而来的,不过P2DR模型中对安全恢复的环节没有足够重视,它把恢复包含在响应环节中,只作为事件响应之后的一项处理措施。PDRR与P2DR相似,唯一的区别就在于把恢复环节提到了和防护检测响应等环

节同等的高度。在 PDRR 模型中，安全策略、防护、检测、响应和恢复(restore)有机结合，共同构成了完整的安全体系，如图 2-2 所示。其中恢复环节对于信息系统和业务活动的生存起着至关重要的作用，组织只有建立并采用完善的恢复计划和机制，其信息系统才能在重大灾难事件中尽快恢复并延续业务。

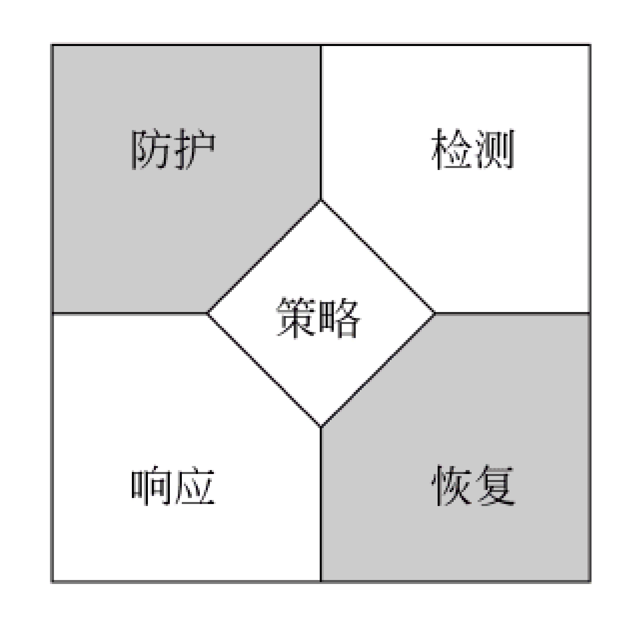



**图 2-2　PDRR 安全模型**

以上模型在网络安全的发展过程中起到了很好的推动与促进作用，由于它们强调了安全技术体系中部分安全要求，忽略了人和管理的因素，因此在具体的实施过程中，很难成为可应用的安全体系架构。由于互联网络的开放性和通信协议的安全缺陷，以及在网络环境中数据信息存储和对其访问与处理的分布性特点，网上传输的数据信息很容易泄露和被破坏，网络受到的安全攻击非常严重，因此建立有效的，可操作的网络安全防范体系就更为迫切。ISO 组织在上述各模型的基础上，在 1989 制定了国际标准 ISO 7498-2—1989《信息处理系统开放系统互连基本参考模型第 2 部分安全体系结构》。

## 2.2.2　ISO 7498-2 安全模型

ISO 7498-2 是一个普遍适用的安全体系结构，该标准为开放系统互连描述了基本参考模型，为协调开发现有的与未来的系统互连标准建立起了一个框架。其任务是提供安全服务与有关机制的一般性描述，确定在参考模型内部可以提供这些服务与机制的位置。按照该标准设计出的不同的安全保障系统，可以满足不同网络环境对安全保密的需要。

ISO 7498-2 中描述了开放系统互连安全的体系结构，提出安全的信息系统的基础架构中应该包含五类安全服务和能够对这五类安全服务提供支持的八类安全机制。五类安全服务即鉴别服务、访问控制、数据完整性、数据保密性和抗抵赖性。八类安全机制包括加密、数字签名、访问控制、数据完整性、鉴别交换、业务流填充、路由控制及公证机制。除此之外，ISO 7498-2 另一个贡献是把这些内容映射到了 ISO 的七层模型中。这个体系结构是国际上重要的安全技术架构，其结构各个部分的关系可以通过如图 2-3 所示的框架结构图表示，其提供的内容包括。

(1) 提供安全体系结构所配备的安全服务和有关安全机制在体系结构下的一般描述。

(2) 确定体系结构内部可以提供相关安全服务的位置。

(3) 保证完全准确地配置安全服务，并且一直维持于信息系统安全的生命周期中，安全功能必须满足一定强度的要求。

框架结构中的每一个系统单元都对应于某一个协议层次，需要采取若干种安全服务才能保证该系统单元的安全。网络层需要有节点之间的认证、访问控制，应用层需要有针对用户的认证、访问控制，需要保证数据传输的完整性、保密性，需要有抗抵赖和审计的功能，需要保证应用系统的可用性和可靠性。

一种安全服务可以通过某种单独的安全机制提供，也可以通过多种安全机制联合提

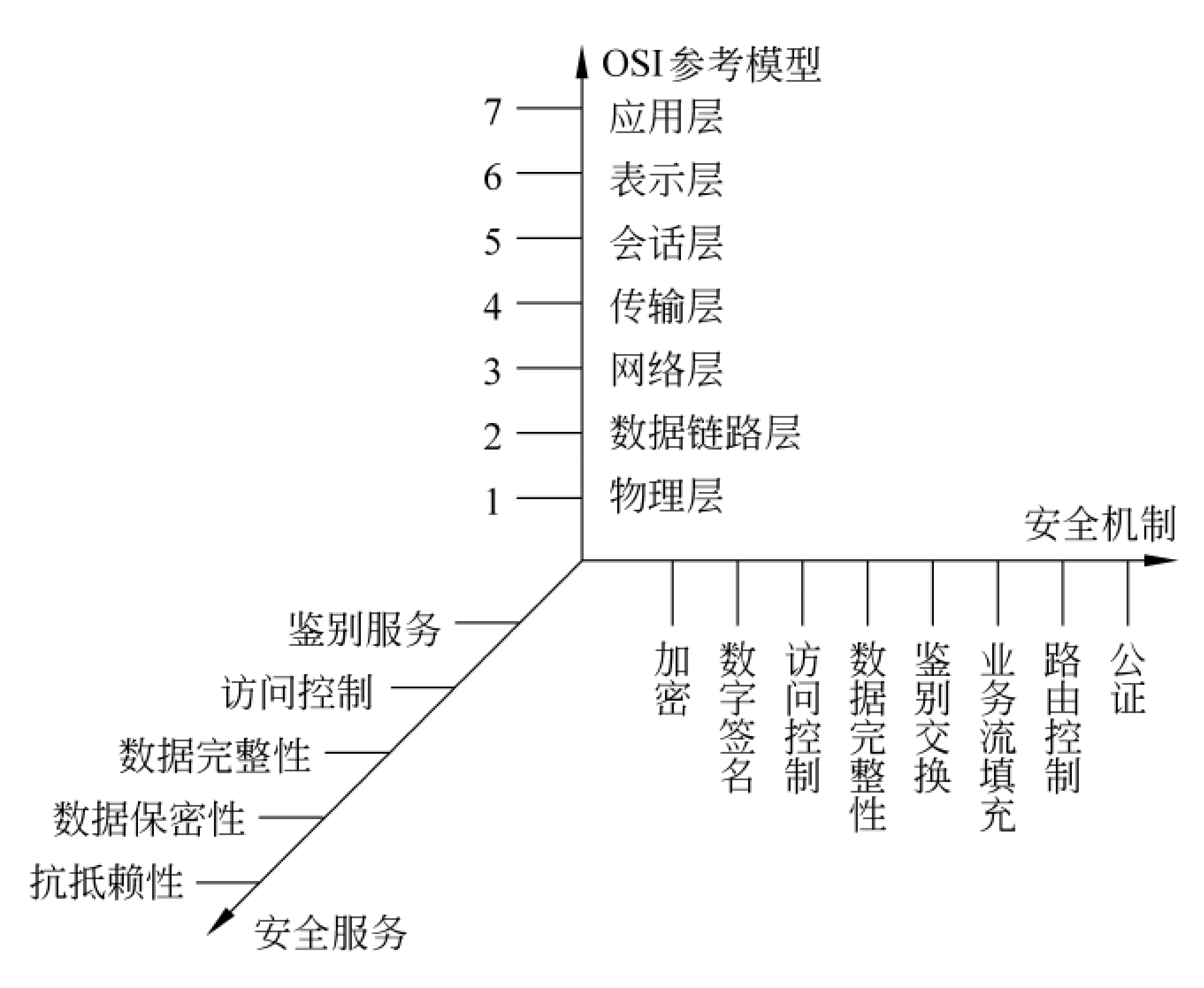



**图 2-3 ISO 7498-2 安全架构模型**

供。一种安全机制可以用于提供一种或多种安全服务。在 OSI 中除了第 5 层以外,每一层均能提供相应的安全服务。实际上,最适合配置安全服务的是在物理层、网络层、传输层以及应用层上,其他层都不适宜配置安全服务。

## 2.2.3 ISO安全体系的安全服务

由于 OSI 网络模型具有开放性和网络协议(如 TCP/IP)本身固有的安全漏洞,以及其他应用系统在实施中产生的漏洞,都会造成许多安全问题并给网络系统带来危害。ISO 7498-2 安全架构针对网络系统存在的潜在威胁提出了五类安全服务。

**1. 鉴别服务(authentication)**

网络上任何两个开放的系统主机在同等分层上建立连接或数据传输过程中对对方实体的合法性进行判断以防假冒。主要分为两部分,一部分是对等实体鉴别服务,用于两个开放系统同等层中的实体建立连接或数据传输阶段,对对方实体的合法性、真实性进行确认,以防假冒,这里的实体可以是用户或进程。另一部分是数据源认证服务,用于确保数据发自真正的源点,防止假冒。

**2. 访问控制(access control)**

访问控制可防止非授权用户非法使用网络资源,以保护网络上特定的数据资源等。它既包括对于用户的身份认证,又包括对于用户的权限确认。这种保护服务不但提供给个人用户,也可以提供给用户组。

**3. 数据完整性(data integrity)**

可防止非法用户对网络上进行交换的数据信息进行更改、插入、删除,以及防止在数

据交换过程中的数据丢失等。主要分为带恢复功能的面向连接方式的数据完整性;不带恢复功能的面向连接方式的数据完整性;选择字段面向连接方式的数据完整性;选择字段无连接方式的数据完整性;无连接方式数据完整性。通过以上这些服务来满足不同用户、不同场合对数据完整性服务的不同要求。

**4. 数据保密性(data confidentiality)**

主要是指保护网上传输的信息及主机之间交换的数据,防止数据信息的泄露和破坏,其中包括多种保密服务。为了防止网络中各个系统之间交换的数据被截获或被非法存取而造成泄密,需提供加密保护。基于 OSI 模型中规定数据传送可采用面向连接的方式和无连接的方式。数据保密还提供用户可选字段的数据保护和信息流安全,即对有可能从检测数据流就能推导出的数据信息提供保护。保证信息流安全的目的是确保信息在从源点到目的地的整个流通过程的安全。一般可通过路由选择使信息流出经由安全路径,并通过信息流量填充来阻止攻击者的信息流量和流向分析攻击。

**5. 抗抵赖性(non-repution)**

这是对数据信息收发双方的行为确认,以防止否认的机制。其主要是保护网络通信不会遭到内部其他合法用户的威胁。它由两部分组成,一是不得否认发送行为;二是不得否认接收行为。抗抵赖性在本质上是一种数字签名服务,它能够提供确定的证据来证明通信双方做过某种操作。

## 224 ISO安全体系的安全机制

为了保证上述安全服务的实现,ISO 提出了以下八种基本的安全机制,通常可以将一个或多个安全机制配置在适当的层次上以实现这些安全服务。

**1. 加密机制(encipherment mechanisms)**

数据保护最主要和最基本的手段就是通过数据加密的方法来实现,也就是通过加密算法来防止数据信息在传输过程中被篡改、删除和替换。用加密的技术结合其他方法,可以提供数据的保密性和完整性。加密算法按密钥类型来划分,可分为对称加密和非对称加密两种;按密码体制可分为序列密码(流密码)和分组密码算法两种。除了会话层不提供加密保护外,加密可在其他各层上进行,与加密机制相伴的是密钥管理机制。

**2. 数字签名机制(digital signature mechanisms)**

数字签名机制是确保数据真实性的基本方法。它采用某种算法,通过对网络传输的信息实现签名,其目的是防止通信双方的任何一方对自己的行为进行否认,以及防止有人冒充通信的一方用户对收到的信息加以篡改或伪造对方发送的信息等。数字签名技术具有解决收发双方纠纷的能力,特别是针对通信双方发生争执时,可能产生的如否认、伪造、冒充和篡改信息等安全问题。

### 3. 访问控制机制(access control mechanisms)

访问控制机制主要用来控制不同用户的访问权限,主要包括用户对网络系统、主机、数据库系统以及文件系统等的访问权限。访问控制机制本质上是一种对资源访问的策略,它把对资源的访问只限于那些被授权的用户。所谓授权就是指资源的所有者或控制者是否允许其他特定的人访问这些资源。访问控制还可以直接支持数据机密性、完整性、可用性以及合法使用的安全要求,它对数据机密性、数据完整性和合法使用所起的作用是十分明显的。访问控制机制可以建立在以下一种或多种手段上。

(1) 访问控制信息库:这里保存有对等实体的访问权限,可以由授权中心保存或者由正被访问的那个实体保存。

(2) 鉴别信息:通过对密码这类信息的占有和出示来证明正在进行访问的实体已被授权。

(3) 权力:通过对其的占有和出示来证明了有权访问由该权力所规定的实体或资源。权力应是不可伪造的并以可信赖的方式进行传送。

(4) 安全标记:当与一个实体相关联时,这种安全标记可用来表示同意或拒绝访问,通常根据安全策略而定。

(5) 访问时间及路由:由安全策略制定对资源的访问时间、持续访问时间以及通过哪条路由进行访问。

### 4. 数据完整性机制(data integrity mechanisms)

因为实体间信息交换是以一种数据单元(包)的形式进行传输的,所以既要对单元数据加密,又要保证数据单元的时序性,以防止篡改、假冒、丢失、重发或插入等。数据完整性包括两种形式,一种是数据单元的完整性;另一种是数据单元序列的完整性。而数据单元完整性包括两个过程,一个过程发生在发送实体;另一个过程发生在接收实体。保证数据完整性的一般方法是发送实体时在一个数据单元上加一个标记,这个标记是数据本身的函数,如一个分组校验或密码校验函数,它本身是经过加密的。接收实体有一个对应的标记,并将所产生的标记与接收的标记相比较,以确定在传输过程中数据是否被修改过,典型的算法有 MD5 和 SHA。

### 5. 鉴别交换机制(authentication mechanisms)

鉴别交换机制是通过互换信息的方式来确认实体身份的机制。在网络环境下,这种认证形式主要有站点认证、报文认证、用户和进程的认证等。用于认证的方法主要有。

(1) 密码:由发送方实体提供,接收方实体检测。

(2) 密码技术:将交换的数据加密,只有合法用户才能解密,得出有意义的明文。在许多情况下,这种技术与时间标记和同步时钟技术、双方或三方“握手”技术、数字签名和公证机构技术一起使用。

(3) 实体的特征或所有权:常采用的技术是指纹识别和身份卡等。

### 6. 业务流填充机制(traffic padding mechanisms)

业务流填充机制是提供业务流机密的一个基本机制。它在信息传输的间隙连续不断发出伪随机序列,使网上窃听者无法判断信息的可用性,并防止其分析信息的流量和流向。它包含生成伪造的通信实例、伪造的数据单元、伪造的数据单元中的数据。伪造通信业务和将协议数据单元填充到一个固定长度,能够为防止通信业务分析提供有限的保护。为了使这种保护得以成功,伪造通信业务级别还必须接近实际通信业务的最高预期等级。另外,协议数据单元的内容必须进行加密或隐藏起来,使虚假业务不会被识别,从而实现与真实业务区分开来。

### 7. 路由控制机制(routing control mechanisms)

在大型复杂的网络中通信的两个节点间可有多条线路,但不是所有线路都安全可靠。在这种情况下,路由控制机制使得路由能被动态的或预期地选取,以便使用物理上安全的子网络、中继或链路来进行通信,保证敏感数据只在具有适当保护级别的路由上传输。另外,如果在检测到持续的攻击时,网络服务提供者可为端系统经不同的路由建立传输。带有某些安全标记的数据可以依据安全策略禁止或允许通过某些子网、中继或链路。连接的发起者可以指定路由选择说明,由它请求回避某些特定的子网、链路或中继。路由控制机制的目的是通过一个公正的仲裁机构,来保证信息传输的路由是安全可靠的。

### 8. 公证机制(notarization mechanisms)

有关在两个或多个实体间通信的数据的性质,如它的完整性、数据源、时间和目的等,能够借助公证机制得到确保。这种保证是由第三方所提供的,公正机构为通信实体所信任,并掌握必要信息,它以一种可证实方式提供所需保证。每个通信实体可使用数字签名、加密和完整性机制以适应公证方提供的服务。当这种公证机制被用到时,数据便在参与通信实体间由受保护的通信实例和公证进行通信。公证机制目的是通过一个公正仲裁机构解决有关信息的责任问题,因此网络上通信的各方都必须由该机构进行数据交换。

以上所讨论的安全服务和安全机制并不是一一对应的,一种安全服务可以采取一种或多种安全机制来实现。在 OSI 网络模型中,一种安全服务是由某一特定层有选择的提供,也就是说安全服务是有相应的安全机制来支持的,表 2-1 给出了与通信协议相关的安全服务(Y 表示提供,N 表示不提供)。

在这种基于 TCP/IP 协议层的网络安全体系结构的指导下,近年来国内外许多网络安全研究机构和生产厂商针对 TCP/IP 协议集各层次上的安全隐患不断推出新的安全协议、安全服务和产品。考查这些网络应用产品,它们在安全的措施与实现上,大都可以在这张表上找到相应的映射。实际上,保障网络安全不但需要参考网络安全的各项标准以形成合理的评估准则,更重要的是必须明确网络安全的框架体系、安全防范的层次结构和系统设计的基本原则,分析网络系统的各个不安全环节,找到安全漏洞,做到有的放矢。

表 2-1　安全服务与 OSI 七层协议的对应关系(深色部分为安全作用区域)

| 安全服务 | 物理层 | 数据链路层 | 网络层 | 传输层 | 会话层 | 表示层 | 应用层 |
|---|---|---|---|---|---|---|---|
| 鉴别服务 | N | N | Y | Y | N | Y | Y |
| 访问控制 | N | N | Y | Y | N | Y | Y |
| 数据加密 | Y | Y | Y | Y | N | Y | Y |
| 数据完整性 | N | N | Y | Y | N | N | Y |
| 抗抵赖性 | N | N | N | N | N | Y | Y |

## 23　TCP/IP的网络安全体系结构

互联网通信是基于 TCP/IP 协议簇的。在 Internet 中,TCP/IP 是互联网通信的事实标准。TCP/IP 协议是一组包括 IP 协议、TCP 协议、UDP 协议、ICMP 协议和其他一些协议的协议组。TCP/IP 协议簇并不完全符合 OSI 的七层参考模型,但与 OSI 模型间存在着特定的映射关系,如图 2-4 所示。

| OSI | TCP/IP | | | | | | |
|---|---|---|---|---|---|---|---|
| 应用层<br>表示层<br>会话层 | 应用层 | HTTP | TELNET | FTP | SMTP | DNS | DHCP | Others |
| 传输层 | 传输层 | TCP | | | UDP | | | |
| 网络层 | 网络层 | ICMP | | | IGMP | | | |
| | | IP | | | | | | |
| | | ARP | | | RARP | | | |
| 数据链路层<br>物理层 | 网络接口层 | Ethernet、FDDI | | | Token Ring | | Others | |

图 2-4　TCP/IP 协议与 OSI 模型的对应关系

传统的 OSI 参考模型是一种通信协议的七层抽象的参考模型,每一层执行某一特定任务。该模型的目的是使各种硬件在相同的层次上相互通信。这七层分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。而 TCP/IP 通信协议采用了 4 层的层次结构,每一层都通过它的下一层所提供的网络来完成自己的需求。TCP/IP 的四层结构如下所示。

(1) 应用层:是 TCP/IP 参考模型的最上层,它是应用程序间沟通的层,为用户访问网络提供一组应用协议,如简单邮件传送协议(SMTP)、文件传送协议(FTP)、网络远程访问协议(Telnet)等。

（2）传输层：传输层提供了节点间的数据传送服务，这一层负责传送数据，并且确定数据已被送达并接收。传输层最常用的有两种协议，一是传输控制协议（TCP）；另一个是用户数据报协议（UDP）。TCP 和 UDP 给数据包加入传输数据并把它传输到下一层中。

（3）网络层：这一层主要解决主机与主机间的通信，在收到报文发送请求后，形成数据包，通过网络接口层将其发出，并对收到的数据包进行处理，形成相应的报文交给传输层，同时解决路由问题，进行差错控制和拥塞控制等。网络层最重要的协议是 IP 协议，其他协议是提供 IP 协议的辅助功能。

（4）网络接口层：对实际的网络媒体的管理，定义如何使用实际网络（如 Ethernet、FDDI、Serial Line 等）来传送数据。

网络攻击总是利用系统中存在的弱点和缺陷，由于 TCP/IP 刚出现时，协议的设计者对网络安全方面考虑较少，随着 Internet 的快速发展，它的各种安全方面的脆弱性逐步体现出来。因此，要理解 Internet 的安全，首先需要对 TCP/IP 中的协议有一个了解，只有这样才能更好地理解 TCP/IP 网络的安全问题。所以下面介绍 TCP/IP 常用的协议组以及每种协议存在的缺点。

## 2.3.1 TCP/IP 协议分析

### 1. IP 协议

Internet 协议（Internet protocol，IP）是基于包的协议，对应于 OSI 的网络层，用于在网络上交换数据。它是一个无连接协议，负责处理地址分配、分段、重装配和协议多路分解，是网络层中最重要的协议，是其他 IP 协议的基础。作为网络层协议，IP 负责地址的分配并负责控制信息以允许数据包在网络中的路由。图 2-5 是 IP 报头的格式（具体参考 RFC791-IP 协议）。

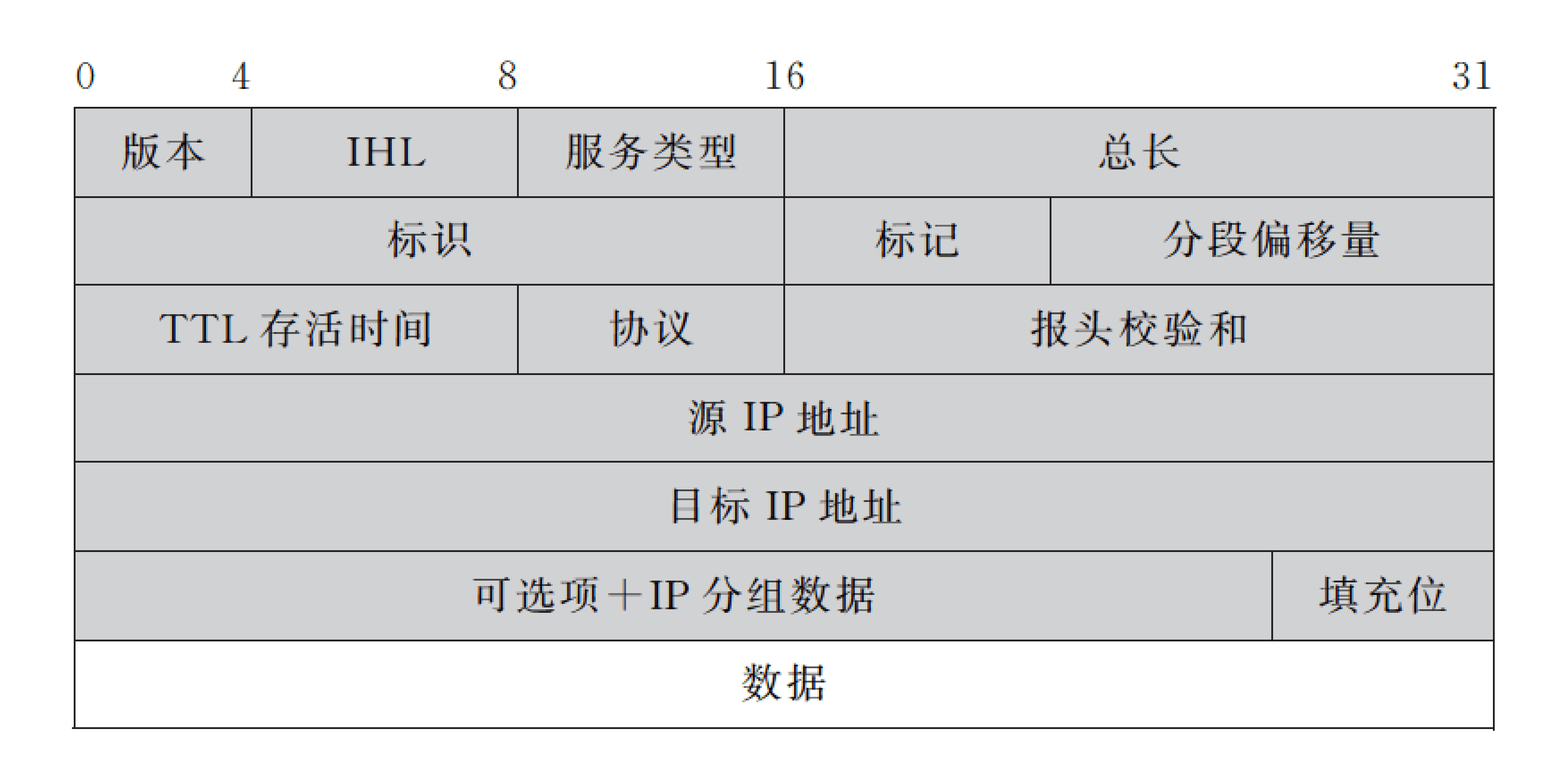



**图 2-5　IP 数据报头格式**

IP 层接收其低层（网络接口层。例如，以太网设备驱动程序）发来的数据包，并把该数据包发送到更高层的 TCP 或 UDP 层。同样，IP 层也把从 TCP 或 UDP 层接收来的数据包传送到更低层。IP 协议是一个无连接的协议，主要的工作就是在主机间寻址并为数

据包设定路由。在交换数据前它并不建立会话,因为它不保证数据的正确传递。另一方面,数据在被收到时,IP 不需要收到确认,所以它是不可靠的。IP 数据包中含有发送它的主机的地址(源地址)和接收它的主机的地址(目的地址)。TCP 和 UDP 服务在接收数据包时,通常假设包中的源地址是有效的。也可以这样说,IP 地址形成了许多服务的认证基础,这些服务相信数据包是从一个有效的主机发送来的。IP 确认包含一个选项,称为 IP source routing,可以用来指定一条源地址和目的地址之间的直接路径。对于一些 TCP 和 UDP 的服务来说,使用了该选项的 IP 包就像是从路径上的最后一个系统传递过来的,而不是来自于它的真实地点。这个选项是为了测试而存在的,说明它可以被用来欺骗系统来进行平常是被禁止的连接。所以许多依靠源地址 IP 做确认的服务会有安全问题,如不采取一些相关的安全措施,将会产生安全问题并且容易被非法入侵。

IP 报头包含如下主要字段。

(1) 源 IP 地址:用 IP 地址确定数据包发送者。

(2) 目标 IP 地址:用 IP 地址确定数据包目标。

(3) 协议:表示上层所使用的协议类型,如 TCP 协议或 UDP 协议。

(4) 校验和:IP 数据每经过一个中间节点都要重新计算校验和,用来证实收到数据包的完整性。

(5) TTL 生存有效时间:指定一个数据报被丢弃之前,在网络上能停留多少时间(以秒计),避免了包在网络中无休止循环。

(6) 可选项:用作对原来设计的补充或新版本的测试及安全措施等,长度最多为 40 字节。

### 2. TCP 协议

传输控制协议(transmission control protocol,TCP)是在 IP 层的基础上构成的,它对应于 OSI 的传输层。它为应用层提供可靠的面向连接的传送服务,规定了数据的格式及数据传输的应答方式。TCP 还规定了计算机验证数据是否可靠到达的过程。TCP 能够将应用程序之间的通信量进行多路分解,所以其允许系统中有多个应用程序同时通信。图 2-6 是 TCP 报头的格式,它以数据部分打头并紧跟在 IP 报头之后。

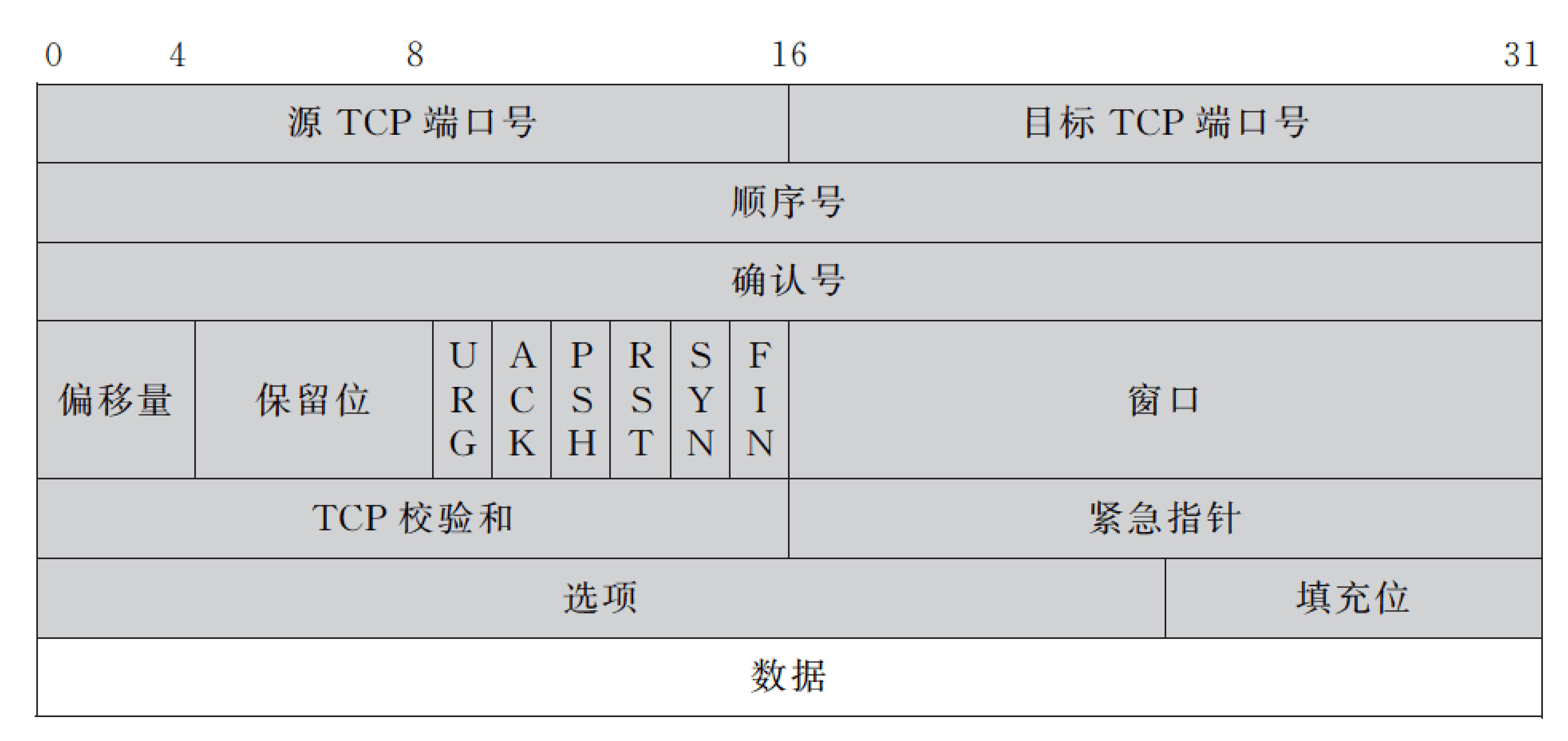



**图 2-6 TCP 报头格式**

TCP 用端口号或套接字(socket)号来向上层传递信息，这种机制能确保协议在端站点的不同进程间进行多路通信。端口号可以跟踪网络中同时进行的不同会话，由操作系统分配。表 2-2 是一些常用的应用服务端口号。

表 2-2 常见端口号

| 应用层 | 端口号 | 应用层 | 端口号 |
|---|---|---|---|
| FTP | 21,22 | HTTP | 80 |
| Telnet | 23 | SSH | 22 |
| SMTP | 25 | HTTPS | 443 |

TCP 报头包含如下主要字段。

(1) 源 TCP 端口号：用于标识报文的返回地址。

(2) 目标 TCP 端口号：用于指明目标的应用程序地址接口。

(3) URG：表示是否使用紧急指针。

(4) ACK：表示请求应答状态。

(5) PSH：表示本段请求入栈。

(6) RST：表示连接复位。

(7) SYN：为同步序号，用来建立连线。

(8) FIN：表示发送方已经发送了最后的字节流。

(9) 校验和：对数据头及封装的包内容进行校验。

(10) 紧急指针：发送紧急数据的一种方式。

TCP 是一种可靠的面向连接的传送服务。它在传送数据时是分段进行的，主机要交换数据必须建立一个会话。它用比特流通信，即数据被作为无结构的字节流。通过为每个 TCP 传输的字段指定顺序号，以获得可靠性。如果一个分段被分解成几个小段，接收主机会知道是否所有小段都已收到。通过发送应答来确认别的主机收到了数据。对于发送的每一个小段，接收主机必须在一个指定的时间返回一个确认。如果发送者未收到确认，数据会被重新发送。如果收到的数据包损坏，接收主机会舍弃它，因为确认未被发送，发送者会重新发送分段。TCP 的建立与释放的步骤如下。

(1) 初始化主机通过一个同步标志置位的数据段发出会话请求。这个请求包中的 SYN 位被置 1，客户机告诉服务器序号字段是有效的，要进行检查。此外，客户机还把 TCP 报头中的序号字段设为初始序号。

(2) 服务器向客户机发送一个包响应客户机的请求，包中的 SYN 位也被置 1，同时服务器初始的序号等于客户机初始序号加 1。

(3) 客户机通过将服务器初始序号加 1 发送出去，表示应答服务器的初始序号。

(4) 建立连接，可以传输数据。

(5) 释放连接，TCP 连接是一个全双工的连接，其接收与释放也需由通信双方共同完成。当通信的一方没有数据发送时，可以将 FIN 报文段发向对方，请求释放连接，只有对方也发送了释放连接请求后，TCP 连接才会完全释放。

TCP 三向沟通的流程如图 2-7 所示。

TCP 端口为信息的传送提供指定地点，小于 256 的端口号被定义为常用端口。TCP 滑动窗口用来暂存两台主机间要传送的数据，有点类似 CACHE。每个 TCP/IP 主机有两个滑动窗口，一个用于接收数据，另一个用于发送数据。窗口大小是 16 位的，接收到的 TCP 最多为 65535 字节。

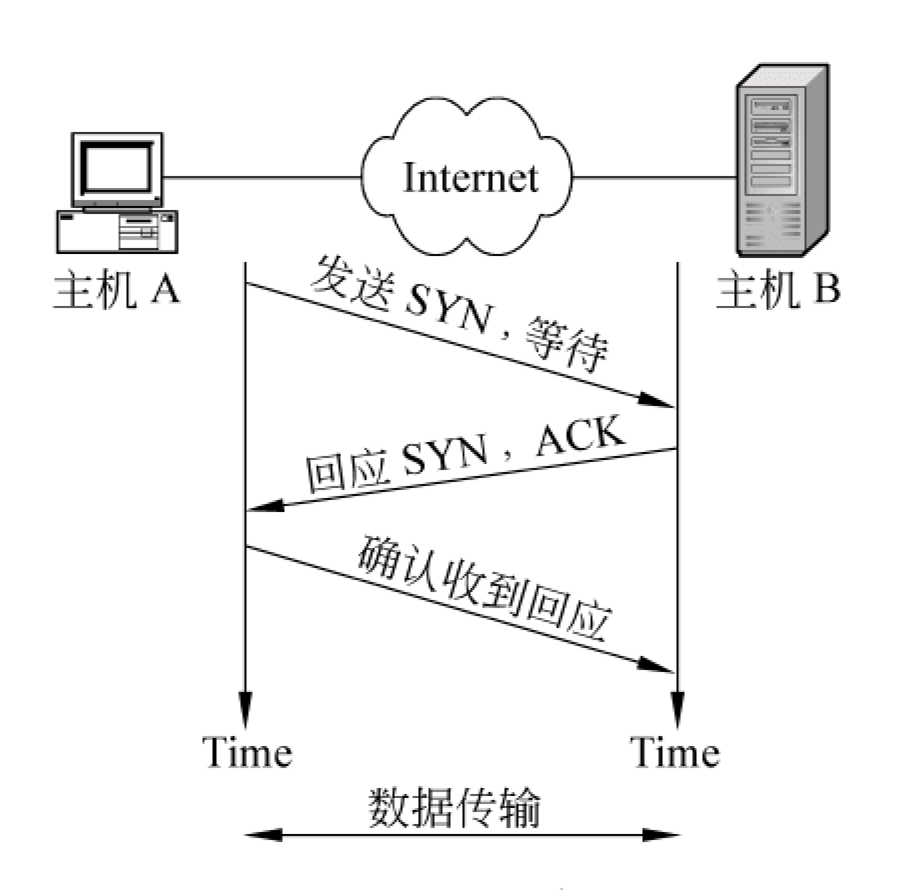



**图 2-7　TCP 三向沟通流程**

### 3. UDP 协议

用户数据报协议（user datagram protocol，UDP）与 TCP 处于同一层，属于传输层协议，它为计算机之间的消息传递提供不可靠、无连接的传输服务。UDP 不提供错误更正和重发，也不能防止包的丢失和重复。因此，它不被应用于那些使用虚电路面向连接的服务，而主要用于那些面向查询/应答的服务，相对于 FTP 或 Telnet，这些服务需要交换的信息量较小。使用 UDP 的服务包括 NTP（网络时间协议）和 DNS（DNS 也使用 TCP）等。图 2-8 给出了 UDP 报头的格式。

0　16　31

| 源 UDP 端口 | 目标 UDP 端口 |
|---|---|
| 报文长度 | 校验和 |
| 数据 | |

**图 2-8　UDP 报头格式**

UDP 包括的字段主要有。

（1）源 UDP 端口：定义了初始化通信的端口号。

（2）目标 UDP 端口：定义了传输的目的端口号。

（3）报文长度：表示 UDP 报文的总长度，包括报头和数据部分的长度。

（4）校验和：对头数据及包的内容进行校验。

欺骗 UDP 包比欺骗 TCP 包更容易，因为 UDP 没有建立初始化连接。也就是说，与 UDP 相关的服务面临着更大的危险。所以，在局域网的入口与出口点设置包过滤指定允许和拒绝基于 UDP 的应用是明智的做法。

### 4. ICMP 协议

因特网控制报文协议（Internet control message protocol，ICMP）与 IP 位于同一层，它被用来报告错误并传送 IP 的控制信息。它主要是用来提供有关通向目的地址的路径信息。ICMP 的“Redirect”信息通知主机通向其他系统更准确的路径，而“Unreachable”信息则指出路径有问题。ICMP 常用于一些流行的网络诊断工具，如 ping 和 traceroute。一个 ICMP 包的封装例子如图 2-9 所示。

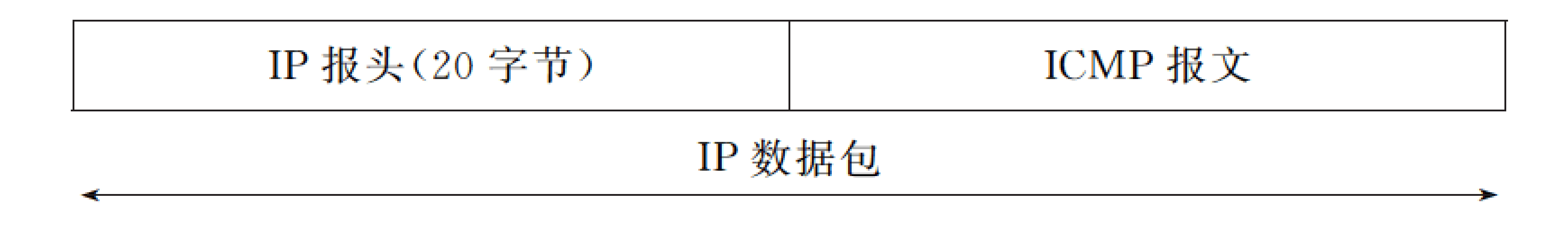



**图 2-9 ICMP 包封装结构**

ICMP 报文是与 IP 包封装在一起的,根据 RFC-791 的说明,IP 包总共可长达 65535($2^{6}-1$)八位组,其中包括报头长度(通常是 20 个八位组,如果不指定 IP 选项的话)。发送方把比 MTU(最大传输单元)还长的包分割成较小的包,然后接收方再把这些分割后的包重新装配。由于其协议具有重组的特征,也常常被用于 Ping of Death、SMURF 攻击。

## 2.3.2 TCP/IP 常见应用层协议分析与应用

### 1. SMTP/ESMTP 协议与应用

Internet 上所有电子邮件都是基于简单邮件传输协议(simple mail transfer protocol,SMTP)的。SMTP 是请求/响应协议,命令和响应都基于 ASCII 文本,并以 CR 和 LF 符结束。响应包括一个表示返回状态的三位数字代码。SMTP 在 TCP 协议 25 端口监听连接请求。ESMTP(Extended SMTP)就是对标准 SMTP 协议进行的扩展。它与 SMTP 服务的区别仅仅是使用 SMTP 发信不需要验证用户账户,而用 ESMTP 发信时服务器会要求用户提供用户名和密码以便验证身份。验证之后的邮件发送过程与 SMTP 方式没有两样。

一旦传送通道建立,SMTP 发送者发送 MAIL 命令指明邮件发送者。如果 SMTP 接收者可以接收邮件则返回 OK 应答,SMTP 发送者再发出 RCPT 命令确认邮件是否收到。如果 SMTP 接收者能收到,则返回 OK 应答。如果不能接收到,则发出拒绝接收应答(但不中止整个邮件操作)。双方将如此重复多次,当接收者收到全部邮件后会接收到特别的序列,如果接收者成功处理了邮件,则返回 OK 应答。

SMTP 提供传送邮件的机制,如果接收方与发送方连接在同一个传送服务下时,邮件可以直接由发送方主机传送到接收方主机。当两者不在同一个传送服务下时,则通过中继 SMTP 服务器传送。为了能够对 SMTP 服务器提供中继能力,它必须拥有最终目的主机地址和邮箱名称。

由于大多数电子邮件程序缺少认证、完整性和机密性服务,因此 SMTP 常受到电子邮件炸弹等攻击。

### 2. FTP 协议与应用

文件传输协议(file transfer protocol,FTP)是基于 TCP 的应用程序,经常用来存储和检索大型数据文件。该协议用了两个 TCP 连接,一个用于初始化控制连接,它由客户端向服务器端发起。另一个用于 FTP 数据连接,它由服务器端发起。大多数常规的 FTP 应用为每个文件传输创建一个新的端口号。这些要求在严格禁止外部发起 FTP 连

接的环境下会遇到问题,包过滤器将阻止从服务器发回的输入数据连接,这将导致文件传输无法进行。为了解决这个问题,开发了被动式 FTP。在这种方式下,控制连接和数据连接都由客户端发起,这样负责包过滤的防火墙将能提供必要的安全保护,但又不会阻挠数据的传输。图 2-10 为 FTP 操作流程。

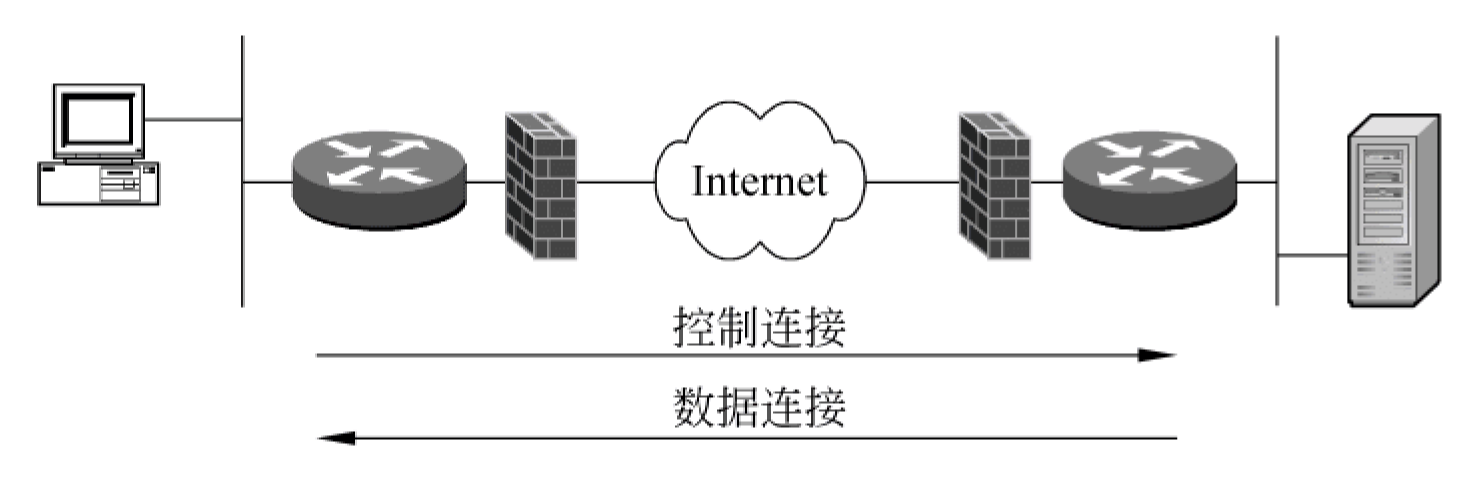



**图 2-10　FTP 操作流程**

### 3. NFS/NIS 服务与应用

网络文件系统(network file system,NFS)和网络信息系统(network information system,NIS)是 UNIX 环境中常用的服务。NFS 用于访问远程文件系统,通过允许安装远程文件系统使他们可以被本地访问。NIS 用于在客户/服务器关系中创建中央服务和数据库。NIS 和 NFS 经常结合使用以帮助强化所装系统的文件许可。NFS 和 NIS 都采用 UDP 作为底层协议。按照典型的配置,在连接的两端仅有有限的认证能力,这些服务是极不可靠的。

## 2.3.3　常见 TCP/IP 安全问题

在理解了 TCP/IP 协议的一些结构安全体系后,下面再讲述一下有关对 TCP/IP 协议簇中的设计漏洞的攻击。一般来说,对于 TCP/IP 的攻击主要包括 IP 地址欺骗、隐蔽通道、IP 分片攻击、连接劫持等方面。

### 1. IP 地址欺骗

在很多攻击类型中,攻击者都会用另一个地址来替换发送者的 IP 地址,IP 欺骗(spoofing)通常被用来突破一个目标主机。此外,IP 欺骗也常被用作发起 DoS(拒绝服务)攻击。攻击者通过修改 IP 分组,误导目标主机,使其以可信任主机方式接受最初的分组。在这个过程中,攻击者必须知道被信任主机的 IP 地址,并且修改分组头部(源 IP 地址),以便让其看起来像是来自被信任的主机。

实施针对某主机的 DoS 攻击时,攻击者并没有兴趣接收来自目标受害者的有效数据或信息,其唯一的目的就是让受攻击的服务器拒绝向其合法用户提供服务,并且不暴露攻击者自己。这样的话,返回地址或者源地址就可以被欺骗。

从上面的 IP 数据报报头格式可以看出,由于缺乏认证,它不能保证数据包的真实来源,这就构成了 IP 欺骗的基础。由于协议的缺陷,到目前还没有理想的方法可以彻底根除 IP 欺骗。只是通过各种手段,尽量减少这种威胁。目前较为理想的方法是使用防火

墙，由防火墙来决定是否允许外部的IP数据包进入局域网，对来自外部的IP数据包进行检验。假如过滤器看到来自外部的数据包说明中有内部的地址，它一定是欺骗包；反之亦然。如果数据包的IP不是防火墙内的任何子网，它就不能离开防火墙。在某种意义上，过滤器分割能将Internet分成小区域。除子网内部外，子网之间不能欺骗。这种方法虽然能够很好地解决问题，但是一些防火墙并不能够正确地区分内部与外部的数据包，并且在实际应用中局域网与局域网之间也常常需要有相互的信任关系以共享资源，这种方案不具备较高的实用价值。

源路由选择是另一种形式的IP欺骗，它利用了IP选项的"源路由选择"(source routing)。"源路由选择"允许发送主机指定目标主机应答时经过的路径。因此，攻击主机时，可以通过源路由选择绕过被冒充的主机，控制远程主机的应答路径选择进行攻击。由于路由器一般配置为禁止源路由选择，因此源路由选择攻击难以实现。

### 2. 隐蔽通道

隐蔽通道(covert channel)可以被认为是两个实体间的一个管道或者通信通道，可被某个进程或者应用程序利用，以违反系统安全规定的方式进行信息传输。对TCP/IP而言，在这种情况下建立隐蔽通道，数据就可以在两个终端系统间秘密地传递。以ICMP为例，在下列环境下，ICMP消息可以提供出错或者控制机制。

(1) 用数据包来测试连接性/可达性，Echo和Echo-Reply消息。

(2) 报告数据包不可到达目的地。

(3) 报告中转数据包出现缓冲区容量问题，源队列消息。

(4) 报告数据包路由路径更改，重定向消息。

ICMP处于TCP/IP协议簇的网络层，可在所有的TCP/IP主机上实现。按照ICMP协议规定，ICMP Echo Request消息应该有一个8字节长的头部和一个56字节长的负载。ICMP Echo Request分组不应该在负载中携带任何数据。不过，此类分组常被用来携带秘密信息。只要稍微改动一下，在ICMP分组负载中携带秘密数据，这可能使得分组更大了，但协议簇本身并没有针对这些问题的控制措施。修改ICMP分组可以入侵者有机会编写特殊的客户端/服务器程序，这些很小的代码能够不经网络管理员注意输出机密信息。阻止超出特定大小限制的ICMP分组是唯一可以避免此漏洞问题的方案。事实上，隐蔽通道普遍存在于TCP/IP协议簇的所有底层协议中。

### 3. IP分片攻击

由于IP协议是允许对数据分组进行分片的，正如前面所述，IP分片偏移用来跟踪同一个数据报的不同部分。此字段中的信息内容可用来在目的地重组数据包。所有此分类分片都有相同的标识字段，分片偏移指明当前分片在整个原始分组中的位置。许多访问服务器和防火墙并不做分组重组，在正常的操作中，IP分片不会相互重叠，但是攻击者可能特意构造分片分组，以误导路由器或防火墙。这些分组通常都很小，因为数据和计算量大，对终端系统来说是很难应付的。这里假定，精心构造的第二个分片分组有一个比之前分片分组长度更小的偏移量，直到数据分组要在目的站点重组，第二个分片会和

第一个分片重叠几个字。这种畸型 IP 分组会影响目的站点操作系统的正常工作，常导致系统崩溃、重新启动、内核转储和其他无法保证的行为。

利用 IP 分片攻击典型的例子是 Ping of Death 攻击。这种攻击发生时，入侵者发送分片，当这些分片在目的地重组时，会产生一个超出最大允许长度的数据分组。这类攻击的一个用途是绕过入侵检测系统的传感器。单个分片并不会匹配任何已知签名(signature)，但当重叠地址覆盖某些数据之后，攻击者就可能被识别。访问路由器和防火墙需要实施恰当的 IP 过滤及配置，确保阻塞此类攻击。这些设备需要对那些具有非零偏移量的分片限定最小偏移量，以防止重叠发生，保证 TCP/IP 程序不发生溢出。

**4. SYN 泛洪**

TCP/IP 协议簇会在整个生命期内使用多个定时器，包括连接建立定时器(connection establishment timer)、FIN_WAIT 定时器和 KEEP_ALIVE 定时器。当开始正常的 TCP 连接时，目的主机将收到一个来自源主机的同步/开始(synchronize/start，SYN)包，并发送一个同步确认(synchronize acknowledge，SYN/ACK)包。目标主机在建立连接之前必须听到对方对 SYN/ACK 的确认(acknowledge，ACK)，这个信息交换过程就是前面介绍的 TCP 的三次握手。在等待对 SYN/ACK 时，目标主机中大小有限的连接队列始终跟踪正在等待完成的连接。该队列通常很快能清空，因为一般在发送出 SYN/ACK 之后的几毫秒之内就能收到 ACK。TCP SYN 攻击利用了 TCP 的这种设计。攻击性的源主机通过用随机源地址向受害主机发送 TCP SYN 包。受害的目的主机将 SYN/ACK 发送回随机源地址，并向连接队列中增加一个条目。由于 SYN/ACK 指定的接收方是不正确或根本不存在的主机，因此三次握手的最后一部分肯定无法完成。于是连接条目将一直保存在连接队列中，直到超时，通常约 1 分钟。如果保持很快的速度通过随机 IP 地址生成假冒的 TCP SYN 包，入侵者就可以把被攻击主机的连接队列填满，使之拒绝为合法用户提供 TCP 服务(如电子邮件、FTP 或 WWW 服务)。

由于源主机的 IP 地址是伪造的，因此很难跟踪攻击的发起者。虽然利用 SYN 攻击可以实现拒绝服务，但是在许多情况下，攻击者都是利用 TCP/IP 设计中的固有缺陷进行攻击，把 SYN 攻击作为其他复杂欺骗和攻击的基础。

作为面向连接的协议，TCP/IP 必须能够适应连接次数的变化，保证一定的连接次数。另外，由于信息在计算机之间来回的时间跨度变化很大，需要充足的时间量来保证连接的顺利建立。然而，只要连接建立持续时间是有限的，其他主机就能向它发送很多不能完成的连接请求，最终阻塞目标主机。这就意味着完全根除 SYN 攻击是非常困难的。通过增加缓存中最大未完成连接的次数(或动态地分配代替固定的最大值)，可以迫使攻击者增加工作量，达到减少攻击的目的。但只要最大未完成连接数是固定的，问题就不能完全解决。

**5. 连接劫持**

连接劫持就是攻击者将自己插入两台主机建立的连接中间并控制连接，是 IP 欺骗的另一种方式。虽然 IP 欺骗不能通过安全认证措施，但是连接劫持攻击却可以在两台

主机间通过认证后，进行数据通信时捕获连接，实施攻击。连接劫持利用同步破坏(desynchronized state)，当接收的数据包的序列号与期望的不同时，称为连接同步破坏。TCP为了通信可靠性，考虑到数据包丢失和网络等待等情况，会造成数据包接收的无序状态，因此使用活动窗口来支持有效通信。这样的话，TCP根据数据包的序列号是否在当前窗口中，决定丢弃还是缓存接收的数据包。当两台主机的同步破坏达到一定程度，它们就相互丢包。接着，攻击者使用带有正确序列号的欺骗包，暗中修改或增加通信命令。但显然，攻击者只有对两台主机的通信进行窃听，才能复制数据包。TCP连接可能会被非授权用户轻易地劫持，以一个Web服务为例进行说明。

如图2-11所示，一个授权用户发送HTTP请求给Web服务器，Web服务器只当来自用户A的分组具有正确的SEQ/ACK号时才会接受。正如前面所述，这些数字对于Web服务器区别不同会话并确保与用户A持续通话非常重要。假定攻击者冒充用户A向Web服务器发送数据分组，有正确的SEQ/ACK组合，Web服务器就会接受这种分组并让ACK号递增。

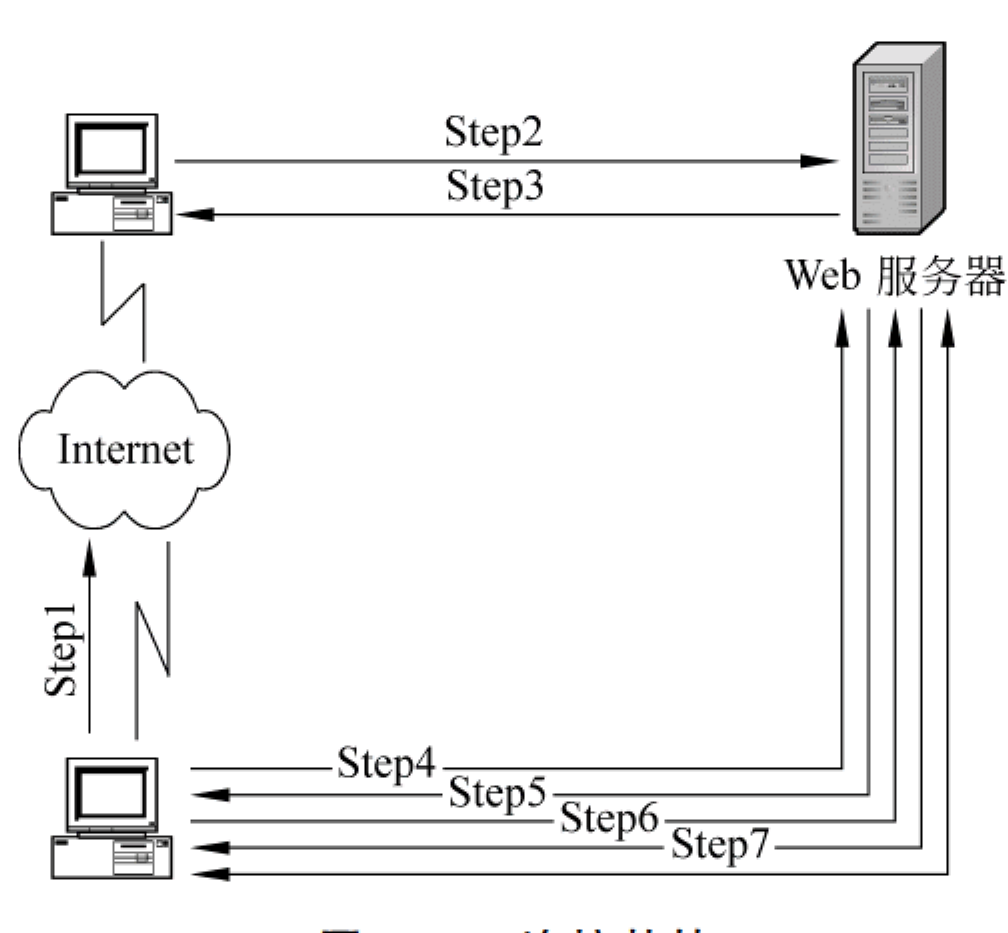



**图 2-11　连接劫持**

与此同时，用户A持续发送数据分组，但SEQ/ACK号已经改变，结果来自用户A的所有不同步的数据分组都会被Web服务器丢弃。攻击者用正确的序列号伪装成用户A，最终导致劫持连接。而用户A却被搞糊涂了，Web服务器会因为攻击者发送正确的同步数据而进行回复。由于连接劫持攻击很难发现，用户A的会话中断，但大多数的网络用户会重新连接会话，认为此事是网络的问题。

### 6. TCP/IP序号攻击

多数TCP/IP程序应用按照可预知的模式来选择序号。当主机执行自引导时，其初始序号为1，初始序号每秒增加128000。因此，如果没有连接发生，32位的初始序号计数器每9.32小时就会循环一次。每发生一次连接初始化，计数器增加64000。如果发生连接时，序号是随机选择的，那么就不能保证所选的序号与前一个不同。正是由于序号不是随机选定的，当攻击者知道序号的选择模式后，就可能发生TCP/IP序号攻击，假冒其他主机，具体过程如图2-12所示。

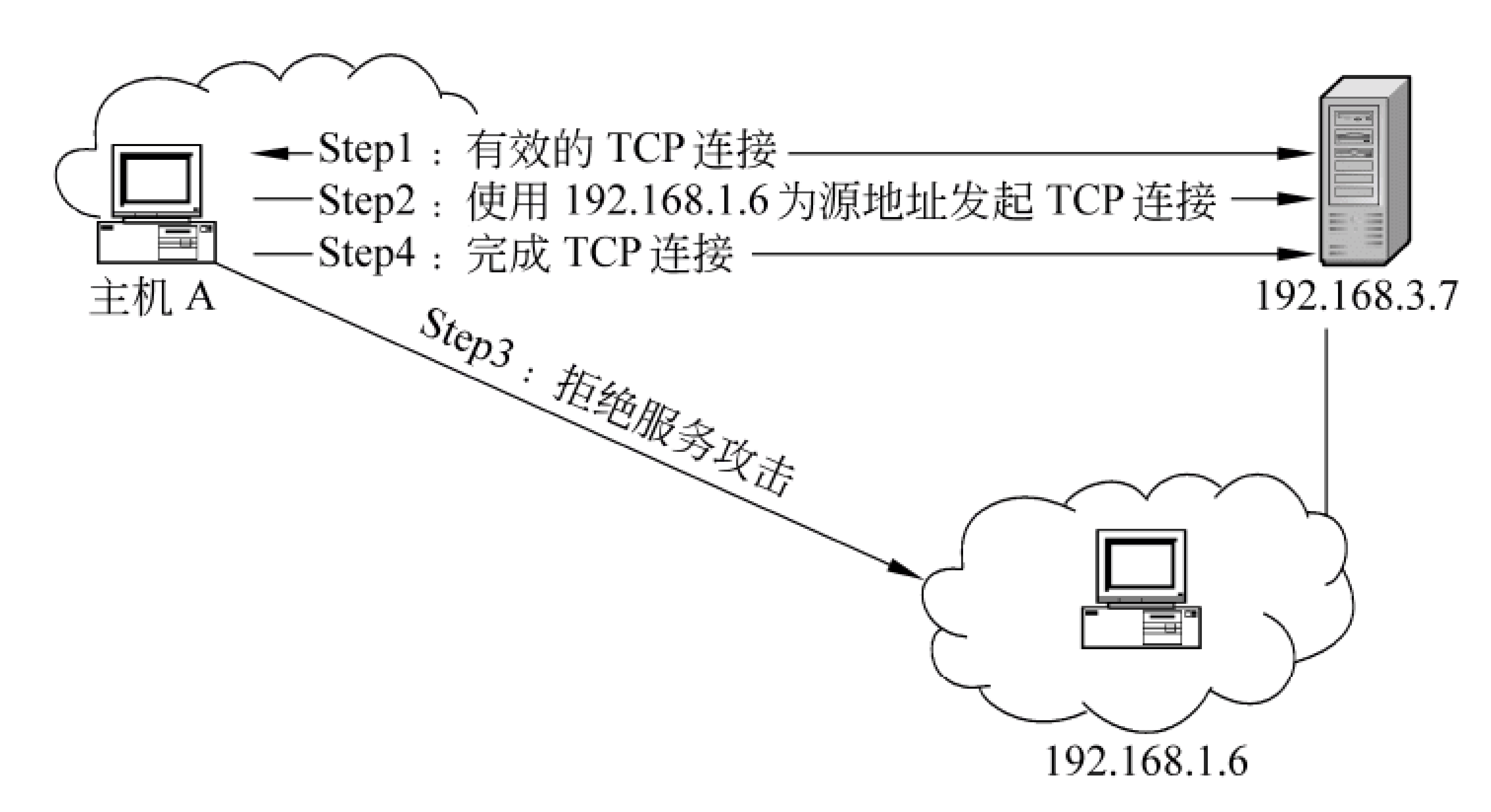



图 2-12 TCP/IP 序号攻击

第一步：攻击者(主机 A)建立到服务器的合法连接并据此判断序号的选择模式。

第二步：攻击者利用服务器信任的主机地址(192.168.1.6)，用假的源地址生成 TCP 连接请求，开始攻击。它在冒充主机的同时还向被冒充的主机发起攻击，使之瘫痪。

第三步：服务器响应连接请求，但由于可信任的主机处于 DoS 攻击下，无法应答。

第四步：攻击者等待一段时间以确保服务器已经答复，然后用猜测的序号给以回应。

如果攻击者推断的序号正确，服务器就会受到安全威胁。无论何时主机 A 和主机 B 进行通信，攻击者可以用正确的序列号复制 A 和 B 的数据包进行发送，当然也能对数据包进行修改。

防止欺骗的最佳方法是在网络的入口和出口点设置包过滤器，外部入口点过滤器明确拒绝所有声称来自内部网络主机的外部数据包。同样，在内部出口点过滤器则只允许来自内部网络主机出去的数据包。

### 7. 连接中的连接失效

若主机 A 和主机 B 已经建立连接，在连接持续期间发送 RST 包将终止连接。要在连接持续期间实现同步破坏，而不终止连接，只需要修改序列号计数器。

实际上，Telnet 协议允许使用 NOP 命令增加接收者的序列号计数器，如果发送足够多的 NOP 命令，攻击者就能实现同步破坏，并用正确的序列号复制数据包。

### 8. 路由(RIP)攻击

“路由信息协议”(RIP)可以在网络中进行路由信息(如最短路径)分配，在广域网上广播路由。和 TCP/IP 一样，RIP 没有认证机制，不能检测 RIP 包上的信息。RIP 攻击与其他攻击不同，它改变了数据的去向，而不是数据的出处。例如，攻击者伪造 RIP 包，宣称他的主机 A 有最快的路径到达其他网络，造成所有从该网络发出的数据包都将经过 A 路由，这时他就可以修改或检查数据包。另外，攻击者也可以假冒任何主机，把所有的网络流量引导到他冒充的主机而不是自己，达到攻击对方的目的。

**9. ICMP 攻击**

IP 层使用 Internet 控制消息协议向远程发送单向消息，例如，ping 命令向远程主机发送 ICMP 的 Echo Request，等待它回送 ICMP 的 Echo Reply 消息。其他 ICMP 消息具有相似的组成。ICMP 没有认证，可以利用 ICMP 进行拒绝服务攻击或进行数据包截取。

拒绝服务攻击使用 ICMP 的“超时”(time exceeded)和“无法访问目标”(destination unreachable)消息。“超时”消息指明 IP 数据报的生存时间(Time-To-Live)已到期，主要由路由循环或到达远程主机过于遥远引起。“无法访问目标”表明数据包不能成功地送达目标主机。这两个 ICMP 消息能引起主机突然终止连接。攻击者利用它，简单伪造“超时”或“无法访问目标”的消息，发送给正在通信的远程主机，远程主机的连接将被终止。

# 2.4 TCP/IP 的安全性改进

由于 TCP/IP 协议安全性的欠缺，对应于 ISO/OSI 的网络安全体系结构，人们采用了在各个层次采取相应的安全协议来处理，这有点类似于打补丁，利用相应的技术来加强与完善 TCP/IP 的安全。根据各个层次的特点，通常采取以下方式来进行安全改进，如图 2-13 所示。

| | |
|---|---|
| 应用层 | SHTTP MOSS PEM<br>PGP<br>SSH Kerberos S/MIME |
| 传输层 | SSL |
| 网络层 | IPSec IPv6 ISAKMP |
| 数据链路层 | |
| 物理层 | |

**图 2-13 TCP/IP 安全协议结构**

## 2.4.1 应用层安全协议

应用层与特定的应用程序有关，而与网络上数据移动的细节联系较少，常见的就是安全超文本传输协议(secure hypertext transfer protocol，SHTTP)。它是一种安全的面向消息的通信协议，设计用于保护使用 HTTP 协议的消息的安全。这种协议保留了 HTTP 的特征，同时允许请求和应答消息被签名、认证、加密或这些方法的任意组合。SHTTP 可以使用“选项协商”来允许客户机与服务器在下列内容上达成一致。

(1) 事务模式：什么内容应该被签名或加密。

(2) 加密算法：使用何种算法来进行签名或加密。

(3) 证书选择：使用哪一种证书。

在实践中,SHTTP 得到的应用并不广泛,对于 Web 安全而言,在传输层处理要更加容易一些。

## 2.4.2 传输层安全协议

安全套接字层协议(secure sockets layer,SSL)是由 Netscape 设计的一种开放协议,它指定了一种应用程序协议(如 HTP、Telnet、FTP)和 TCP/IP 间提供数据安全性分层的机制,为 TCP/IP 连接提供数据加密、服务器认证、消息完整性以及可选的客户机认证。SSL 的主要目标是在两个通信应用程序间提供私密性和可靠性,这个过程由以下三个元素来完成。

### 1. 握手协议

此协议负责协商被用于客户机和服务器之间会话的加密参数。当一个 SSL 客户机和服务器第一次开始通信时,它们在一个协议版本上达成一致,选择加密算法,选择相互认证,并使用公钥技术来生成共享密钥。

### 2. 记录协议

这个协议用于交换应用层数据。应用程序消息被分割成可管理的数据块,还可以压缩,并应用一个 MAC(消息认证代码)。然后结果被加密并传输,接受方接受数据并对它解密,校验 MAC,解压缩并重新组合它,再把结果提交给应用程序协议。

### 3. 警告协议

这个协议用于指示在什么时候发生了错误或两个主机之间的会话在什么时候终止。

安全套接字层协议(SSL)的最大优点是它提供了连接安全,其具有三个基本属性。

(1) 连接是私有的。在初始握手定义了一个密钥之后,将使用加密算法。对于数据加密使用对称加密(如 DES 和 RC4)。

(2) 可以使用非对称加密或公钥加密(如 RSA 和 DSS)来验证对等实体的身份。

(3) 连接时可靠的。消息传输使用一个密钥的 MAC,包括了消息完整性检查。其中使用了散列函数(如 SHA 和 MD5)来进行 MAC 计算。

下面来看一个使用 Web 客户机和服务器的范例,如图 2-14 所示。Web 客户机通过连接到一个支持 SSL 的服务器,启动一次 SSL 会话。支持 SSL 的典型 Web 服务器在一个与标准 HTTP 请求(默认为端口 80)不同的端口(默认为 443)上接受 SSL 连接请求。当客户机连接到这个端口上时,它将启动一次建立 SSL 会话的沟通。当沟通完成之后,通信内容被加密,并且执行消息完整性检查,直到 SSL 会话过期。SSL 创建一个会话,在此期间沟通必须只发生过一次。

第一步:SSL 客户机连接到 SSL 服务器,并要求服务器验证它自身的身份。

第二步:服务器通过发送它的数字证书证明其身份。这个交换还可以包括整个证书链,直到某个根证书权威机构(CA)。通过检查有效日期并确认证书包含有可信任 CA 的数字签名,来验证证书。

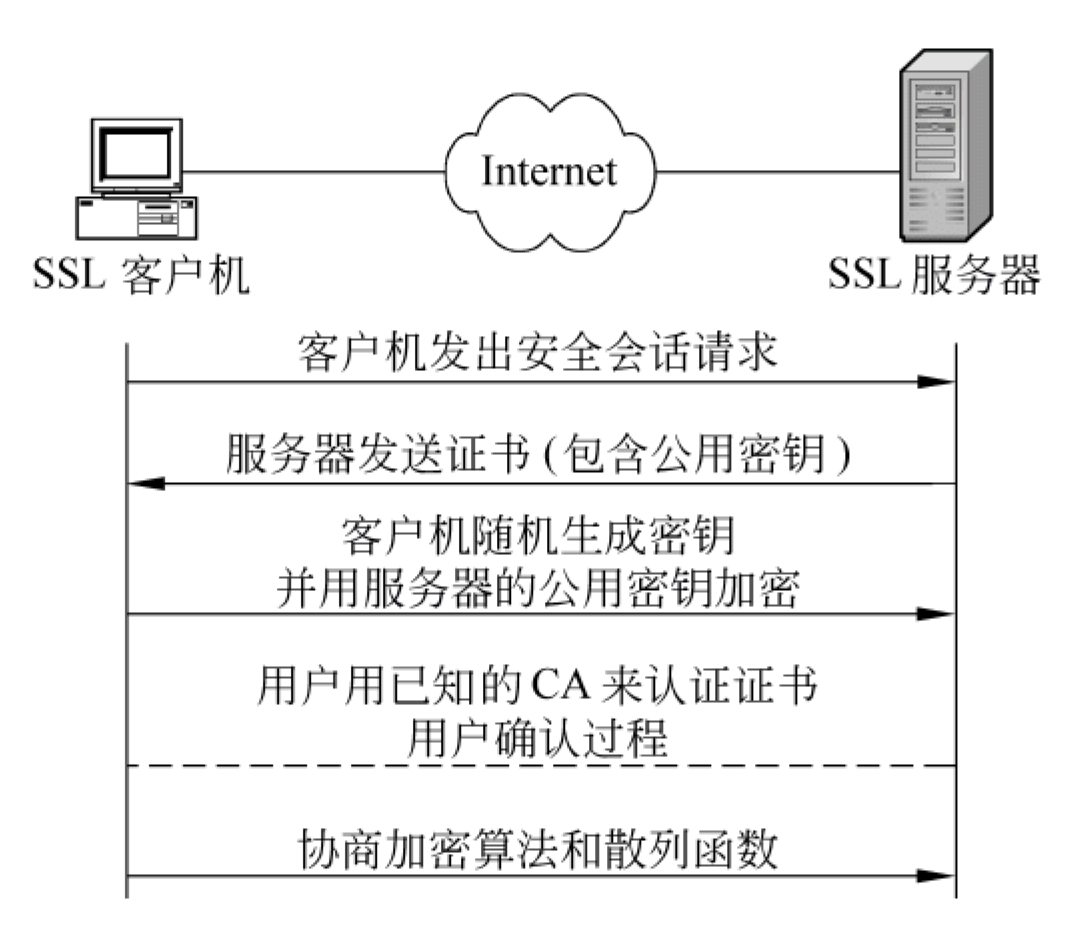



**图 2-14 SSL 握手过程步骤**

第三步：服务器发出一个请求，对客户端的证书进行验证。但是，因为缺乏公钥体系结构，当今的大多数服务器不进行客户端认证。

第四步：协商用于加密的消息加密算法和用于完整性检查的散列函数。通常由客户机提供它支持的所有算法列表，然后由服务器选择最强健的加密算法。

第五步：客户机和服务器通过下列步骤生成会话密钥。

(1) 客户机生成一个随机数，并使用服务器的公钥(从服务器的证书中获得)对它加密，并发送到服务器上。

(2) 服务器用更加随机的数据(客户机的密钥可用时则使用客户机密钥，否则以明文方式发送数据)响应。

(3) 使用散列函数，从随机数据生成密钥。

对于 SSL 的接受程度仅仅限于 HTTP 内。尽管在其他协议中已被证明可以使用，但还不成熟，并没有被广泛应用。IETF 正在定义一种新的协议，叫做“传输层安全”(transfer layer security，TLS)。它建立在 Netscape 所提出的 SSL 3.0 协议规范基础上，但是在 TLS 和 SSL 3.0 之间存在着显著的差别(主要是它们所支持的加密算法不同)，所以 TLS 1.0 和 SSL 3.0 不能互操作。

## 2.4.3 网络层安全

网络层安全是指在 TCP/IP 协议栈的 IP 层上的安全性服务，主要包括 IP 安全协议(IP security，IPSec)套件。它由一套标准组成，用于在 IP 层上提供保密性和认证服务。为了确保在任何 IP 网络上拥有安全的私密通信，也为了整合不同标准及不同厂商产品，IETF 着手制定了一套开放标准网络安全协议 IPSec(IP security)。它将密码技术应用在网络层，以提供传送、接收端做数据的认证(authentication)、完整性(integrity)、存取控制(access control)以及机密性(confidentiality)等安全服务，高层的应用协议也可以直接或间接地使用这些安全服务。

IPSec 是设计来达到网络层中端到端安全通信的第三层协议，它主要的架构是 IP 认

证标头（authentication heade，AH）以及 IP 封装安全装载（encapsulating security payload，ESP）。IP AH 提供数据的完整性和认证，但不包括机密性，而 IP ESP 原则上只提供机密性，但也可以在 ESP Header 中制定适当的算法及模式来确保数据的完整性并得到认证，IP AH 和 IP ESP 可以分开使用或一起使用。完整的 IPSec 还应包括 IP AH 和 IP ESP 中所使用密钥的交换和管理，也就是安全群组（security assocication，SA）和密钥管理（Internet key exchange，IKE）。由于 IPSec 应用广泛，下面对这些内容做一下简单论述。

### 1. 认证头（authentication header，AH）

IP AH 需要使用 128 位的 MD5 计算出整个数据的散列函数值，使得接收端也可以验证、计算是否使用了相同的密钥以检查数据是否正确完整，若检查不符则将此数据包丢弃。将这个头添加到 IP 数据包中后，将确保数据完整性和数据源认证，包括外部 IP 头中的不变字段。

### 2. 封装安全有效载荷（encapsulating security payload，ESP）

IP ESP 标准描述如何加密 IP 的装载数据（payload），加密的范围可以是整个 IP 数据包或只是上层 TCP、UDP 或 ICMP 数据。IP ESP 所使用的保密技术是数据保密标准（data encryption standard，DES）或 Triple-DES，模式则是加密区块链（cipher block chain，CBC）。除了加密以外，IP ESP 也能应用在认证 、完整性以及防止攻击上。

在 IPSec 中，不管是 IP AH 或 IP ESP 均有两种不同的操作模式，隧道模式（tunneling mode）及传输模式（transport mode）。

### 3. 隧道模式（tunneling mode）

隧道用于给定网络的入口点和出口点把数据包封装到一个可以理解的协议中，这些入口点与出口点被定义成“隧道接口”。隧道模式可以被数据包端点和中间安全网关支持。对于 ESP 而言，首先使用 SA 的相关信息将 IP 的数据包加密（含 IP 标头），接下来在前面加上 ESP Header。然后 Prepend 新的 IP 标头。接收端收到 ESP 数据包后，使用 ESP Header 内容中的 SPI 值决定 SA，然后解出 ESP Header 后的装载数据，就可以取回原始的 IP 标头与数据包，可以继续地往下传，如图 2-15 所示。

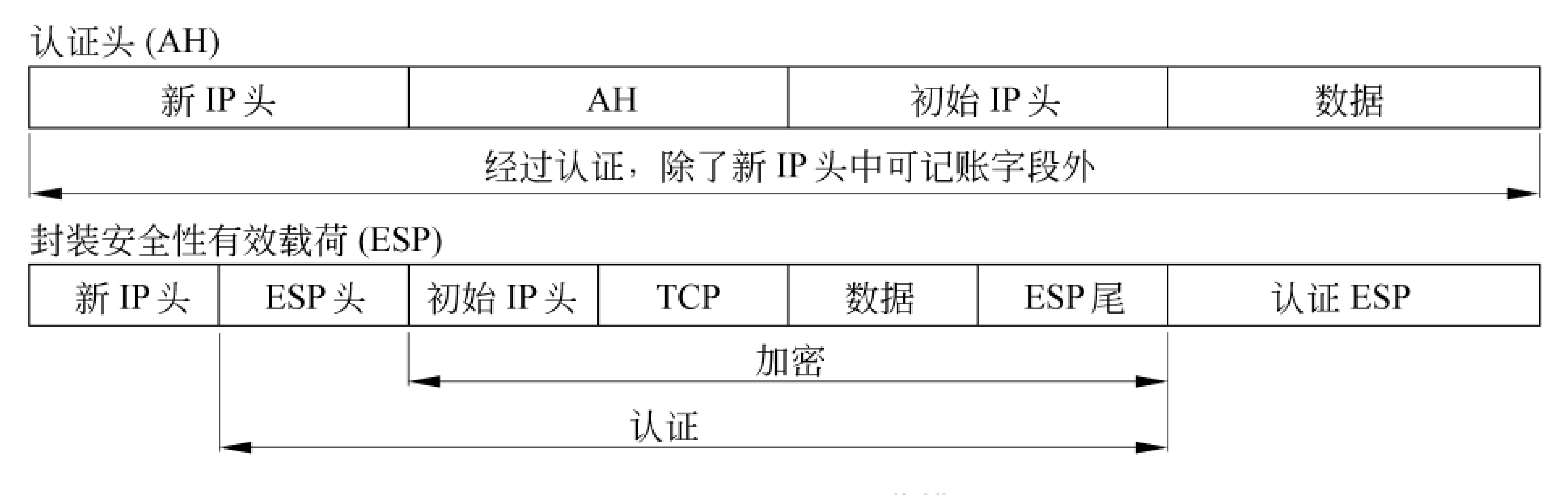



图 2-15 IPSec 隧道模式

如果在隧道模式下使用AH,则外部IP头的一部分被保护以及隧道中的所有IP数据包受到保护。如果使用ESP,则将只保护隧道中的数据包,而不保护外部头。

**4. 传输模式(transport mode)**

在这种模式中,两个主机主要为上层协议提供保护,加密端点是数据包的源和目的地。在IPv4中,传输模式安全协议头出现在IP头之后,并且位于任何高层协议之前,这个过程如图2-16所示。

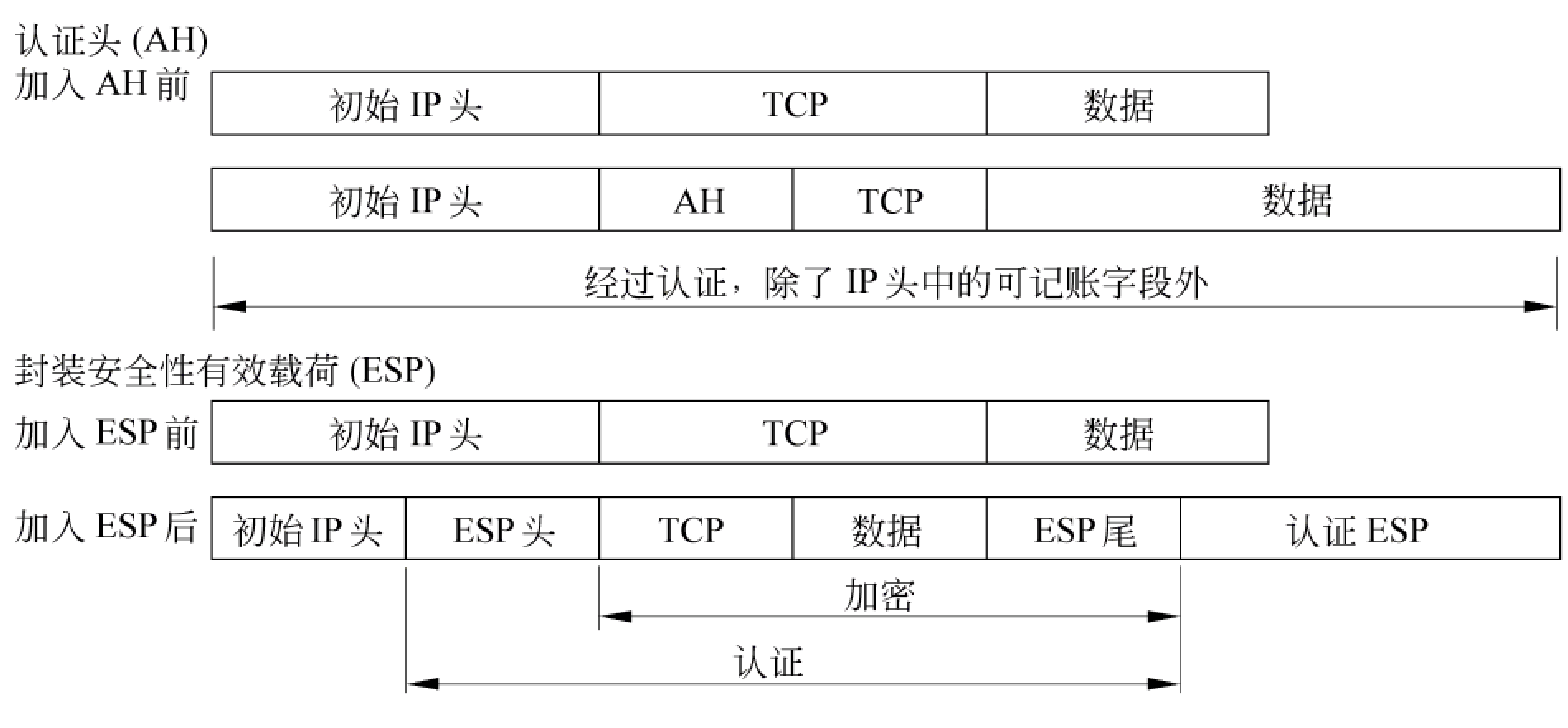



**图2-16 IPSec传输模式**

在IP AH的传输模式下,所有上层信息都得到保护,并且IPv4头中所有字段一般都在传输途中修改。在IP ESP的传送模式下,只为高层协议提供安全服务,ESP标头直接加在欲传送的数据前,这种模式可节省带宽。因为IP标头不需加密,所以不像隧道模式,一个数据包中有两个IP标头。首先将IP装载数据使用ESP封装起来(ESP Header和ESP Trailer),发送端利用使用者ID和目的端地址得到SA环境,然后用加密算法(DES或Triple-DES)加密传送的数据。接收端接收到ESP封装的数据包时直接处理IP标头(因为没有加密),然后从ESP Header拿取SPI值以得到相对的SA,再利用SA的安全环境所订的解密函数解出所加密的资料。对传送模式而言,解密的人就是目的地端的使用者。但是针对Firewall、Gateway Proxy而言,使用隧道模式则较为合适,因为它们并不是原始的传送接收端。IP AH与IP ESP可以独立或分开使用。数据认证之前作加密的好处是对认证数据也有加密,因此,没有人可以更改认证数据。

在IPSec标准中最重要的项目就是安全关联(security association,SA),它定义了一个安全的“环境”。这个环境的内容包含了IP数据包加密、解密和认证的相关信息,叙述如下。

(1) 密码功能:提供加密、认证或两者同时。

(2) 密码算法:如加/解密使用DES(或Triple-DES)、认证使用MD5(或SHA-1)。

(3) 密码算法中所使用的密钥,密钥的生命周期等。

(4) 是否有初始化向量。

(5) SA的生命周期。

SA 可以使用安全参数索引 SPI(32 位)来描述,也就是一个 SPI 值决定一个特定的 SA,而主机的 IP 地址与 SPI 则定义了唯一的 SA。例如,主机 A 可以通知主机 B,SPI 值为 1000,它所相对的 SA 环境,用 DES 加密,密钥为 0x1234567890abcdef(长度 64 位)。主机 A 就可以利用 SPI 1000 的值来加密它的数据,然后传送到主机 B。当 B 收到数据包后利用主机 A 和 SPI 的值就可以决定出 SA 而解密取回原始数据。

从上面的叙述可以发现 SA 是单向的(A-B),但是对主机 A 与主机 B 这两个要建立安全通信的主机而言则需要两个 SA,(A-B)和(B-A),每一个方向一个。此外 SA 的使用有两种键入方式,主机导向键入方式(host-oriented keying)与使用者导向键入方式。前者是不考虑使用者,从同一个系统所发出的数据包,均使用相同的密钥,而后者则是以使用者为参考,允许使用者有不同的密钥。例如,同一使用者有多把密钥用于不同的服务,如 FTP 与 Telnet 使用不同的密钥。

IPSec 采用加密密钥用于认证、完整性和加密服务,在 IP AH 和 IP ESP 中所用到的认证与加密密钥,如何交换与管理呢? 它支持手工密钥分发,也支持自动密钥分发。手工密钥的管理方式是由某个人输入与和其他系统安全通信有关的内容和 SA 管理数据,从而手工配置每一个系统。手工技术只能用在小规划的静态环境中,如果主机数一多,或是主机数据经常更改,此时就需要一套安全且正式的协议来做这件事情了。目前主要的密钥管理协议的参考规范有 SKIP(simple key-management for IP)和 ISAKMP/Oakley(Internet security association and key management protocol /Oakley)。上述两种方法都可应用在 IPv4 与 IPv6 中,SKIP 较为简单,而 ISAKMP/Oakley 则可以应用于较多的协议。事实上,IP 层的密钥交换协议还有 Photuris 和 SKEME 等。

**5. SKIP**

它是由 Sun Microsystem 所发展,目前有三种版本:Sun,TIK 和 ELVIS+SKIP。SKIP 密钥管理的观念是阶层式的密钥管理。通信的双方真正共享的密钥是 Kij(这是利用 Diffie Hellman 的公开密钥对而达到共享的)。为了安全的考虑,公开密钥应到凭证管理中心申请凭证。因此,IPSec 的使用也需要每一国家的公开密钥基础建设(Public Key Infrastructure,PKI)来配合。SKIP 原来想和 ISAKMP 整合,但失败了。因为 IPv6 已决定使用 ISAKMP 与 Oakley 密钥交换的合并协议,也就是 ISAKMP/Oakley(Internet key exchange, IKE)。所以 SKIP 并非 IPSec 强制规定的密钥管理方法。

**6. IKE**

它被选择用于 IPSec 的默认“自动密钥管理协议”是 Internet 密钥管理协议(Internet key management protocol, IKMP),现在简称为 Intetnet 密钥交换(Internet key exchange,IKE)。IKE 将认证 IPSec 中所涉及的每一个对等实体,协商安全策略,并处理会话密钥交换。IKE 是一种混合协议,是 ISAKMP 使用 Oakley 的一些模式和 SKEME 快速 rekey 的观念合并而成,以一种安全的认证方式协商并派生出 SA 的密钥内容。

**7. ISAKMP**

ISAKMP(Internet security association and key management protocol)是 Internet 安全联合和密钥管理协议。它为认证和密钥交换提供了一个框架,但没有定义它们。ISAKMP 被设计成与密钥交换无关。ISAKMP 有两个操作阶段。第一阶段中,相关的一些安全属性经过协商,并产生一些密钥。这些内容构成第一个 SA,一般称做 ISAKMP SA。与 IPSec SA 不一样的是它是双向的。第二阶段则是以 ISAKMP SA 的安全环境来建立 AH 或 ESP 的 SA。也就是说,它支持许多不同的密钥交换。

**8. SKEMI 和 Oakley**

Internet 安全密钥交换机制(secure key exchange mechanism for Internet, SKEMI),它描述了一种功能多样的密钥交换技术,这种技术提供匿名、否认性和快速密钥刷新功能。Oakley 则是由亚利桑那大学所提出的,它与 SKEME 有相当多的共同部分,描述了一系列密钥交换,并详细阐述了每种模式所提供的服务。

IKE 在两个实体间建立一个认证的安全通道,然后为 IPSec 协商安全联合。当协商了有关属性(加密算法及认证方法等)后,双方都需要相互进行认证。IKE 支持多种认证方式,通常会使用以下机制。

(1) 预共享密钥。把同一个密钥预先安装在每一台主机上。IKE 对等实体通过计算一个包含预先共享密钥数据的加密散列值来相互认证。如果接收实体可以使用其预先共享密钥创建相同的散列值,则它知道双方一定是共享相同的密钥,从而验证了另一方的身份。

(2) 公钥加密。每一方生成一个伪随机数,使用另一方的公钥对它及其 ID 加密。每一方都具有计算包含其他对等实体的伪随机数和 ID 加密散列值的能力,用本地私钥解密后相互验证了实体的身份。

(3) 数字签名。每个设备以数字形式对数据集签名,并把它发送给其他方,有点类似于公钥加密方法,但它提供了"不可否认"功能。

数字签名和公钥加密方法都需要使用数字证书来证实公钥/私钥映射。IKE 允许独立地访问证书,或让两个设备显式地交换证书作为 IKE 的一部分。当完成 IPSec SA 的建立后,就可以用协商得到的 IPSec 参数进行数据交换了,图 2-17 描述了 IPSec 保护数据流的创建的过程。

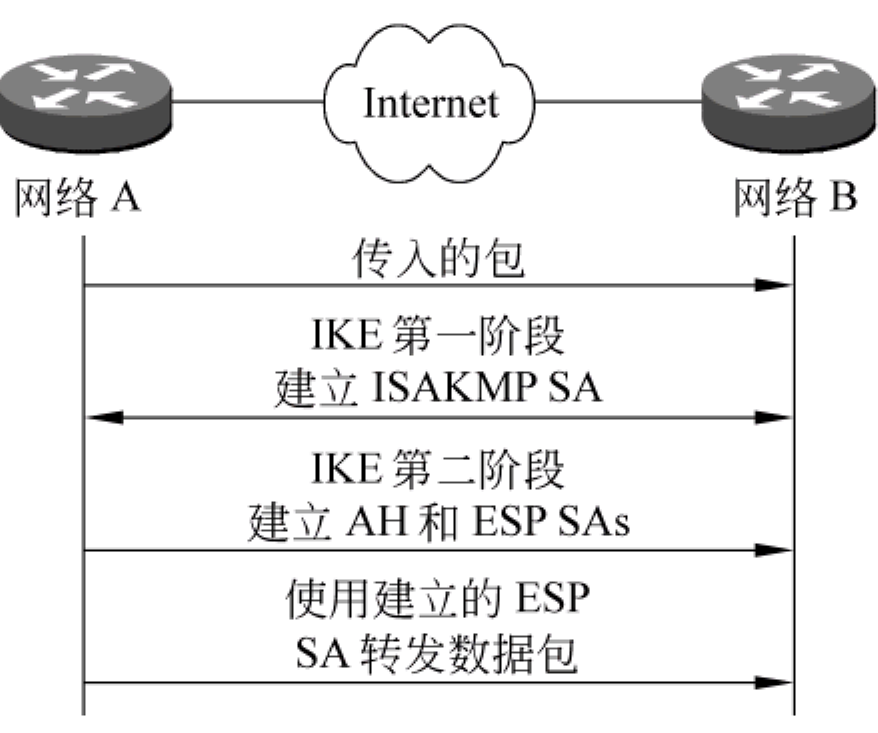



**图 2-17 建立 IPSec 数据保护**

## 2.4.4 使用 TCP/IP 层中的安全性

在给定环境中所使用的安全协议取决于所需要的安全服务以及需要保护的应用。

应用层安全协议的优点是可以根据应用的活动来定义特殊的安全服务。如对于Web,可以对不同的Web页采用不同的安全措施。在传输层安全中,所有的应用消息都必需相同处理。SSL已经被普遍接受,并且被大量部署在WWW环境中;SSH被大量用于安全远程登录和远程文件传送中。通过使用IPSec的网络层可以在IP层上定义安全服务。具有隐藏传输层信息的优点,并且还可以支持除TCP外的其他传输层协议。一般情况下,需要组合使用安全协议,其中大多数环境下都使用某些传输层协议和IPSec的组合。

通过上述对目前国内外安全体系结构和安全标准体系的研究分析,使用户对整个安全体系结构的认识进一步加深和清晰化。网络安全是一个综合多交叉的学科领域,涉及数学、电子、通信、计算机等学科。由于Internet的迅速发展,对于网络系统的攻击数量与日俱增,更多的人都意识到了暗藏在身边的很多漏洞。本章分析了网络安全体系的发展过程,对TCP/IP协议进行了初步的分析,介绍了由于网络体系结构的弱点而造成的一些网络安全问题,并指出了为保证一定程度上的网络安全,应该在哪些层次上采取相应的措施。

## 习 题 2

(1) 简述ISO 7498-2网络安全体系结构。

(2) TCP/IP协议与OSI有哪些区别?详细说明TCP/IP协议各层的特点与应用。

(3) 常见的TCP/IP的安全问题有哪些?如何改进TCP/IP的安全?

(4) 请结合一个防火墙产品的实例来分析其工作原理及安全体系。

(5) 如何理解网络协议安全的脆弱性?

# 第 3 章 chapter 3

# 网络安全策略及实施

网络安全是一个系统工程，用户需要对网络所面临的威胁进行风险评估，决定其需要的安全服务种类，并选择相应的安全机制，然后集成先进的安全技术，形成一个全方位的安全系统。在实施网络安全的过程中，不仅要靠先进的技术，还需要严格的制度管理、法律约束以及用户安全教育等。先进的技术是网络安全的根本保证，严格的安全管理是确保安全策略落实的基础。各网络使用机构应建立相应的网络安全管理办法，强化内部管理，建立合适的网络安全管理体系，加强用户管理和授权管理，建立安全审计和跟踪体系，以此提高整体网络安全意识。此外还需要有严格的法律、法规来保障网络安全。由于计算机网络发展迅速，相关的法律法规比较滞后，许多行为无法可依、无章可循，从而导致网络上的侵害事件不断增多。面对日趋严重的网络犯罪，必须加快建立与完善有关法律法规。

## 3.1 安全策略概述

解决网络安全问题，技术是主体，管理是灵魂。只有将有效的安全管理自始至终贯彻落实于网络安全体系当中，网络安全的可靠性、长期性和稳定性才能有所保证。而要进行有效的网络安全管理，必须根据需要建立起一套科学的、系统全面的网络安全管理体系，即网络安全策略。安全策略处于整个网络安全体系的核心，它可以是一个对网络系统能使用的策略，也可以是相关内容的详细文件。

### 3.1.1 安全策略的定义

网络安全策略可以简单地认为是一个对网络相关各种资源进行可接受使用的策略，也可以是关于连接要素和相关内容的详细文件。根据 RFC2196 的定义，“安全策略是对访问规则的正式陈述，所有需要访问某个机构的技术和信息准资产的人员都应该遵守这些规则”。因此，安全策略本质上就是一个文件，该文件对如何使用与保护计算机网络及其资源进行了概括，它规定了网络安全状态的一个基准线，为网络安全实施设定了一个目标框架。安全策略为实现网络基础设施的安全性提供安全框架，详细定义了用户允许及禁止的行为，确定了实施网络安全必要的工具和程序，对网络安全达成一致意见并由

此定义各种角色，并规定了发生网络安全事件后的处理程序与方法，必要时可为法律行为提供依据。

一个企事业单位的安全策略的内容，从宏观的角度反映了该单位整体的安全思想和观念。一般而言，安全策略需要由高级管理部门负责制定，来确保网络系统运行在一种合理的安全状态下，既能满足安全需要，又不得妨碍员工和其他用户从事正常的工作。这种安全策略对于网络安全体系的建设和管理起着举足轻重的作用。所有网络安全建设的工作其实都是围绕安全策略展开的，它是制定具体策略规划的基础，并为所有其他安全策略标明应该遵循的指导方针。而这些具体的策略内容则可以通过安全标准、安全方针、安全措施等来实现。安全策略是整个安全体系的基础，而安全标准、安全方针、安全措施是安全体系的框架，在这个安全框架中使用必要的安全组件、安全机制等提供全面的安全规划和安全架构。其中安全标准是强制性执行的，它规定了硬件、软件产品应当如何使用，并提供方法手段来保证网络中应用程序、特定技术等以规定的方式执行。而安全方针则指出了当安全标准中未对不可预料的情形定义时的补充规定。安全措施则指出了在操作环境中安全策略、安全标准、安全方针的具体的实现步骤。

### 3.1.2 安全策略的内容

安全策略的目标是让用户和管理层等能够意识到各自在保护组织技术和信息资产方面的责任。它需要阐述一种机制，使每一个成员都面对同样的规则，以便于每个成员都能明白自己在保护网络和信息安全方面的责任，理解自己在网络中能够做什么以及不可以做什么。所以安全策略应当尽可能明确清晰，避免出现容易使人误解的内容，从而对网络安全造成隐患。一个好的安全策略，涉及的内容相当广泛，但总体而言，应当具备如下一些关键内容。

(1) 权威的声明和效力范围：用以识别安全策略的发起者和覆盖的主题范围。

(2) 物理安全策略包括环境安全、设备安全、媒体安全、信息资产的物理分布、人员的访问控制、审计记录、异常情况的追查等。

(3) 网络安全策略包括网络拓扑结构、网络设备的管理、网络安全访问措施(防火墙、入侵检测系统、VPN等)、安全扫描、远程访问、不同级别网络的访问控制方式、识别/认证机制等。它规定了组织内部用户关于网络访问能力的规范。

(4) 数据加密策略包括加密算法、适用范围、密钥交换和管理等。

(5) 数据备份策略包括适用范围、备份方式、备份频率，备份数据的安全存储、负责人等。

(6) 病毒防护策略包括防病毒软件的安装、配置、对软盘使用、网络下载等做出的规定等。

(7) 应用系统安全策略包括WWW访问策略、内部邮件与外部邮件的访问策略，数据库系统安全策略、应用服务器系统安全策略、个人桌面系统安全策略、其他业务相关系统安全策略等。

(8) 身份识别与认证策略：用来规定用什么样的技术和设备来确保只有授权的用户才能访问组织的信息与数据，包括认证及授权机制、方式、审计记录等。

(9) 灾难恢复与应急响应策略：用来规定如何建立安全事件响应小组，如何针对突发事件采取的响应措施，包括响应小组、联系方式、事故处理计划、控制过程、恢复机制、方式、归档管理、硬件、软件等。主要工作有保护机构的系统与信息，还原操作，起诉入侵者，减少损失等。

(10) 密码管理策略包括密码管理方式、密码设置规则、密码适应规则等。

(11) 补丁管理策略包括软件升级、系统补丁的更新、测试、安装等。

(12) 系统变更控制策略包括对设备更新、软件配置、控制措施、数据变更管理、一致性管理等。

(13) 商业伙伴、客户关系策略包括合同条款安全策略、客户服务安全建议等。

(14) 复查审计策略包括对安全策略的定期复查与审计。

(15) 安全教育策略包括安全策略的发布宣传、执行效果的监督、安全技能的培训、安全意识教育等。

(16) 对安全控制及过程的重新评估、对系统日志记录的审计、对安全技术发展的跟踪等。

网络安全策略的内容一般是由以上一系列安全策略文件所涵盖的，文件的繁简程度与网络的规模及应用有关，其中部分内容是多数网络安全都需要且应该制定并执行的。这些安全策略文件的内容应当遵守相关的法律法规，在对网络及其信息资源进行保护的同时，也要注意对工作人员的隐私保护。

### 3.1.3 网络安全模型

在建立合适的安全策略之后，必须从方法上考虑把安全策略作为正常网络操作中的一部分，并把这种描述转化为具体的操作，如对路由器进行配置，安装防火墙，配置入侵检测系统，开发认证服务器和加密的 VPN 等。当开发并制定了安全策略后，就可以选用各种产品，采用各种技术方法来进行具体的实施。但在此之前，还需要全面了解用户需求、需要保护的内容以及网络拓扑结构。开发并保护网络的过程可以采用图 3-1 来说明，这个被称为网络安全模型。

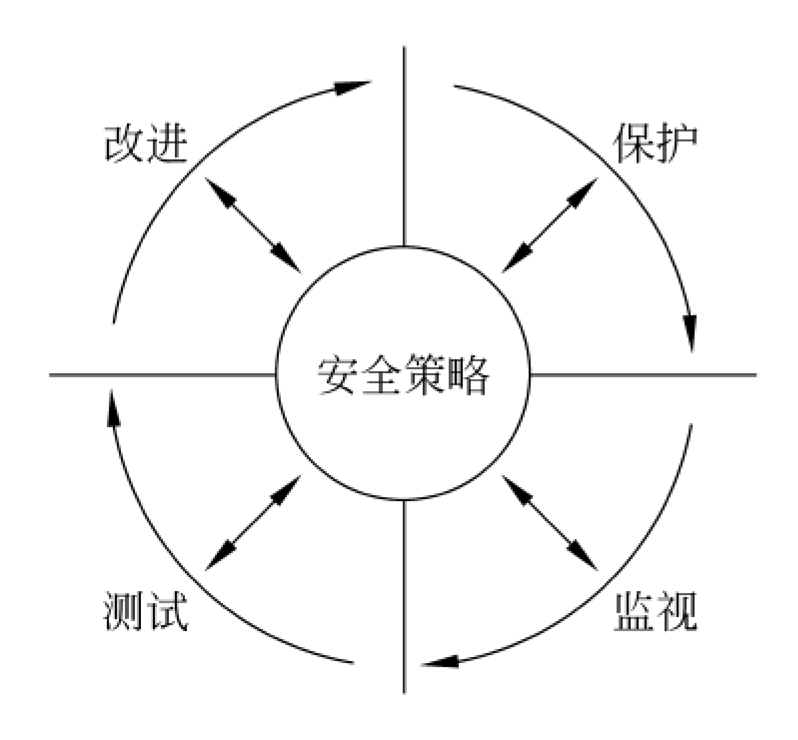


**图 3-1 网络安全模型**

从网络安全模型图上可以看出，安全策略处于网络安全模型的核心，它规定了网络系统中的各个实体在安全方面的技术要求，并定义了网络系统及管理员应该如何配置系统的安全性。由于这种配置还会影响用户，所以还需要针对策略中声明的某些要求，要求管理员与用户进行沟通，再根据用户的需求修改安全策略。在这个网络安全模型中，一共分为四个阶段，每个阶段的侧重点都不同，但是所有的工作都围绕着安全策略来进行的，下面对各个阶段详细说明。

### 1. 保护阶段

在保护阶段，由负责组织安全的人员或部门实施安全解决方案以阻止或预防非授权访问，可采用的方法包括。

(1) 身份认证和验证。这种方法规定了系统用户和管理员的主要认证机制，对每个用户身份、位置和确切登录时间的识别与映射，规定了密码的最小长度、密码的最长和最短使用期限以及对密码内容的要求等。身份认证一般和网络服务授权关联在一起。

(2) 访问控制。主要指对文件实施的访问控制标准要求，一般需要指定两项要求，一是机制和文件的默认要求，对于计算机系统中的每个文件都应该有用户的访问控制措施。该机制应该与认证机制配合工作，以确保只有授权用户才能访问文件。二是机制本身至少应该指定哪些用户可以对文件拥有读、写和执行的权限。

(3) 数据加密。这是一种确保网络数据通信的保密性、完整性和真实性的方法。规定在机构中使用的加密方法，可用的加密方法很多，包括 DES、3DES 和 AES 等。对于安全策略而言，没有理由规定只采用一种算法。当然，这里还需要规定密钥管理所需要的相关程序。

(4) 防火墙。防火墙可以是置于网络上的一套关联设备，用它来保护私有网络的资源，使其免遭外网用户访问。防火墙也可能是一个或多个独立设备，甚至可以在大多数路由器上配置而成。从防火墙技术诞生以来，它作为一种有效的访问控制设备，在防范网络入侵和恶意行为方面起到了关键作用。

(5) 漏洞补丁。这种方法规定安全程序应该在何处查找恶意代码，可以保证识别并弥补可能的安全漏洞。这些漏洞可能会让网络失控，导致信息被随意使用。安全策略应该规定这种安全程序的要求，可以包括这种安全程序要检查的特定文件类型，以及当文件打开时检查文件或按计划检查文件这类要求。

### 2. 监视阶段

围绕着安全策略，在实现了网络系统的安全技术措施后，接下来必须对网络系统进行监控，确保安全状态能够保持，对于所部署的这些安全系统需要加以更频繁的注意。如果不对网络进行安全监控，则在上一步所实施的这些安全措施就没有实际意义了，所以在这个阶段，系统管理员需要通过利用网络漏洞扫描器，定期对网络进行扫描监控，以便可以预先识别漏洞区域，进行漏洞的修补。还可以通过 IDS 系统，对正在发生的安全事件进行监视并响应。经过这个阶段，就能对当前网络上传输的数据流有一个清晰的判断，使对当前网络的认知达到一个新的状态。

### 3. 测试阶段

监视阶段之后是测试过程，对网络系统安全进行测试与进行安全监视一样重要。没有测试，就不能知道现有的和最新的攻击方式，就无法模拟受到安全侵害后的及时响应。由于入侵者是一个不断变化的，具有高度技术能力的群体，如果单靠用户来进行测试，会具有相当的难度，而且实施的成本较高，需要高度的技术支撑。如果用户没有这种技术

体系来支持，最好能委托第三方的专业队伍来对系统进行全面的安全测试，选择那些可提供实际数据进行分析，以提供给用户相对完整的测试报告与安全建议。

**4. 改进过程**

用户应该利用监视和测试阶段得来的数据去改进安全措施，并根据识别的漏洞和风险对安全策略加以调整。系统改进可确保得到最新的安全修复。由于网络安全不是一个静态的过程，经过网络安全改进阶段后，系统又重新进入了新的保护阶段。

通过网络安全模型，可以看出网络安全是一个围绕安全策略而开展的持续不断的过程。一个完善的网络安全策略需要经过多次修改进行逐步完善，而不是一个一劳安逸的过程。不过，安全策略本身不用为不同的操作系统或应用规定专门的配置方法，这项工作应该由特定的配置过程去完成。对于特定的这种配置过程及内容可以被安排在安全策略的附件中，而不是在策略本身中。安全策略并不是一个系统的具体的操作手册，具体的实施方案与内容应由更具体的文件来规定。

## 3.2 网络安全策略设计与实施

安全策略的制定是比较烦琐和复杂的工作，许多安全策略将重点放在了有效实施的概念上，这种观点的出发点在于，如果策略无法得到实施，那么制定的策略再好也没有可用之处。从安全系统的设计人员的角度看，重要的是理解实施策略有若干不同的方式，而具体的实施过程并不属于安全系统的设计人员的考虑范围。所以，由于用户对网络的具体需求不同，可能会包含不同的设计与实施要求。根据前面讨论的安全策略的相关内容，从大的方面来说，一般需要包括物理安全控制、逻辑安全控制、基础设备和数据完整性、数据保密性、用户行为控制以及安全意识培养等几个部分。

### 3.2.1 物理安全控制

物理安全控制是指对物理基础设施、物理设备的安全和访问的控制。对于网络而言，这部分相对变化较少，是最容易被管理员忽略的。对于网络系统，如果为了适应已经变化的环境而正在创建或修改安全策略，就有必要根据安全需求更改物理基础设施，或改变某些关键设备的物理位置，以使安全策略更容易实施。如果已经将物理安全控制与安全策略相结合，那么当用户需要扩充和增加新的应用时，也应该在创建新的应用的同时考虑网络的物理安全控制。

物理网络基础设施包括选择适当的介质类型及电缆的铺设路线，其目的是要确保入侵者无法窃听网络上传输的数据，并且保证所有关键系统具备高度可用性。从安全角度看，由于光纤对于防止传统的网络窃听很有效果，在工程上得到了大量应用。而对于双绞线和同轴电缆，利用一些工具就可以方便进行信号窃听。然而，以目前这种网络环境而言，已经很少出现对线路物理上进行分隔与窃听的行为了。在大多数的情况下，入侵者只需找到一台联网的已授权的计算机，就可以方便地对网络资源进行非法的享用了。

所以对网络设计而言,在物理安全控制上需要更多考虑的是网络拓扑结构,其中还涉及网络及其附属设备的可用性以及网络基础设施的可靠性和安全性。设计出优秀的网络拓扑结构,对于降低安全风险有重要作用,如单点的故障,突然停机等,一个好的网络拓扑可以有效遏制安全事故。

此外,网络资源的存放位置也极为重要,所有网络设施都应该放置在严格限制来访人员的地方,以降低出现非法访问的可能性。特别是涉及核心任务与机密信息的一些设备,这些基础设备包括交换机、路由器、防火墙以及提供各种网络应用与服务的服务器。对于这些设备,在制定安全策略的时候,要考虑对设备区域的授权访问。不但要保证物理安全策略的可强制执行,还需要确保员工的工作地点不与访问限制冲突。为保护关键的网络资源,必须安装和充分的使用环境安全防护。系统越关键,需要设置的安全防护就越多,应不惜任何代价确保资源可用,包括环境安全保护(如火灾、水灾的预防、检测和保护),温度与湿度的控制,保护不受自然灾害及过量磁场的干扰等。

### 3.2.2 逻辑安全控制

逻辑安全控制是指在不同网段之间构造逻辑边界,同时还对不同网段之间的数据流量进行控制。逻辑访问控制通过对不同网段间的通信进行逻辑过滤来提供安全保障。对内部网络进行子网划分是进行逻辑安全控制的有效方法。由于子网由本地负责管理,从网络外部看到的是一个单独的大网络,入侵者对其内部子网的划分没有太详细的了解。但事实上,在网络内部,每个子网都按照实际的物理布线组成各自的 LAN。根据网络如何使用子网来进行逻辑划分,以及这些子网之间的通信如何进行控制,就可以大致判定网络的逻辑设施。一般是由三层交换机(路由选择)来决定如何从不同的网络上访问数据,虚拟局域网(VLAN)也能够修改传统的物理边界。

路由策略是安全策略的重要组成成分,安全策略中可以体现详细的路由安全策略。在路由策略中,通常根据实际的需要来发布和接收被分隔开的网络和子网的路由。如果不考虑所用的路由协议,大多数路由器都禁止发布特定的路由,并将接收到的这类路由忽略,不将它们放到路由地址表中。实现这一目的的方法通常很多,最好是先设计逻辑边界,确定环境所需要的开放或封闭程度,然后再执行相应的路由策略。

VLAN 用于将相关的单个用户组织成新的组,并不考虑用户主机到网络的实际物理连接,它是一种逻辑上的连接。这些相关用户可以分布在内部网络的不同网段上,甚至也可以分布在各地。用户分组的策略很多,如可以根据用户所在部门或工作组来划分。分组的方法一般是要将用户划分到不同的 VLAN 中,这样大多数的用户通信量将在 VLAN 内部进行。如果一个 VLAN 中不包括任何的路由器信息,则该 VLAN 用户只能在本 VLAN 间通信,而不能与本 VLAN 外的其他 VLAN 用户通信。一般情况下,一个 VLAN 可以对应一个特殊的子网,由于 VLAN 可以把位于不同网段的网络终端归类成组,所以必须保证 VLAN 的边界易于理解和配置。

由于逻辑安全不如物理边界那么安全,所以必需完全理解数据从一点传输到另一点的详细路径。尽管在不同的子网之间通常存在逻辑边界,但路由策略和 VLAN 的不当使用常常会使逻辑通信变得混乱。而且在进行逻辑控制过程中,由于很容易实现 IP 欺

骗攻击,因此,采用某种过滤方式最好与其他安全措施结合使用。检测网络上非授权通信的唯一方法是采用数据包分析仪或入侵检测系统(IDS),如果可能尽量在关键的网络访问点上安装入侵检测系统。

对于设备和网段的访问必须明确限制到需要访问的个人,为此需要执行两类控制。一是预防性控制,用于识别每个授权用户并拒绝非授权用户的访问。二是探测性控制,用于记录和报告授权用户的行为,以及记录和报告非授权的访问,或者对系统、程序和数据的访问企图。这就要求必须遵守正确的技术方案,尽量在实际使用中让用户身份验证方法和可对系统提供足够安全的方法之间取得平衡。

### 3.2.3 基础设施和数据完整性

在网络基础设施中,必须尽力保证网络上所有通信都是有效通信。为保证网络间的通信,当前常见的安全防护系统包括防火墙、入侵检测系统、漏洞扫描系统、安全审计系统、病毒防护系统等。

#### 1. 防火墙

防火墙通常被用来进行网络安全边界的防护。事实证明,在内网中不同安全级别的安全域之间采用防火墙进行安全防护,不但能保证各安全域之间相对安全,同时对于网络日常运行中各安全域中访问权限的调整也提供了便利条件。

#### 2. 入侵检测系统

入侵检测系统在网络中的部署很大程度上弥补了防火墙防外不防内的特性,同时对网络内部的信息做到了实时的监控和预警。入侵检测系统与防火墙的联动给内部网络中重要的网络资源打造了一个动态的实时防护屏障。

#### 3. 安全审计系统

利用安全审计系统的记录功能,对网络中出现的操作和数据等做详细的记录,为事后攻击事件的分析提供有力的原始依据。

#### 4. 病毒防护系统

利用网关型防病毒系统可将病毒尽最大可能的拦截在网络外部,同时在网络内部采用全方位的网络防病毒客户端进行全网的病毒防护。针对服务器采用专有的服务器防病毒客户端,同时保证全网病毒防护系统做到统一管理和统一的病毒防护策略。

如何保证有效通信,对于网络服务和协议的选择是一项复杂而艰巨的任务。一个简单的方法就是先允许所有类型的服务和协议,然后再按需要把某些类型取消。这种处理方法实施起来比较方便,因为所需要做的只是启动所有服务并允许其在网络中通行,当出现安全漏洞时,就在主机或网络层次上限制出现漏洞的服务或为服务添加补丁。当然,从安全的角度讲,另一种更安全的方法是先拒绝所有类型的服务和协议,然后按照具体要求开放所需的服务。这需要对各类协议与服务有很清晰的理解,才能更好地分析判

断哪些协议或服务是用户所需的,并根据网络应用的要求,制定出与开放相适应的安全机制。

为了确保数据完整性,对于大多数跨网段的通信需要进行验证,同时为了确保网络基础设施的完整性,对安全基础设施进行操作的通信也应该通过验证。例如,路由表的更新等。如果不对这种信息更新进行验证,未授权的或者恶意的路由更新消息就会危及网络通信的安全。在实际应用过程中,常采用校验和的方式来验证路由更新消息,以保证路由的安全。

### 3.2.4 数据保密性

数据保密性是指保证网络实体间通信数据的保密,使其不能被非法修改,它属于加密的范畴。在加密技术中,最困难的部分是确定哪些数据需要加密,以及哪些数据不需要加密。这个过程应该使用风险分析步骤来进行决策。在风险分析中,可以将不同敏感程度的数据进行分类,对于不同的类别要求制定相应的数据保密措施。在一个网络基础设施内,是否需要加密通信在很大程度上取决于信息的敏感程度和数据被窃取的可能性。在许多环境下,敏感数据的加密多数发生在接入访问点和 Internet 访问点之间。而在网络基础设施中,特别是在访问设备信息时,机密性也是十分重要的。设备之间的通信主要有 Telnet 会话、TFTP 下载配置、SNMP 与网络设备间的通信以及对设备信息的 HTTP 访问等。图 3-2 显示了一些基础设施可能需要加密的通信,可以利用 SSH 和 IPSec 等来提供这些支持,具体选择哪种技术主要取决于各种产品是否支持这项技术。

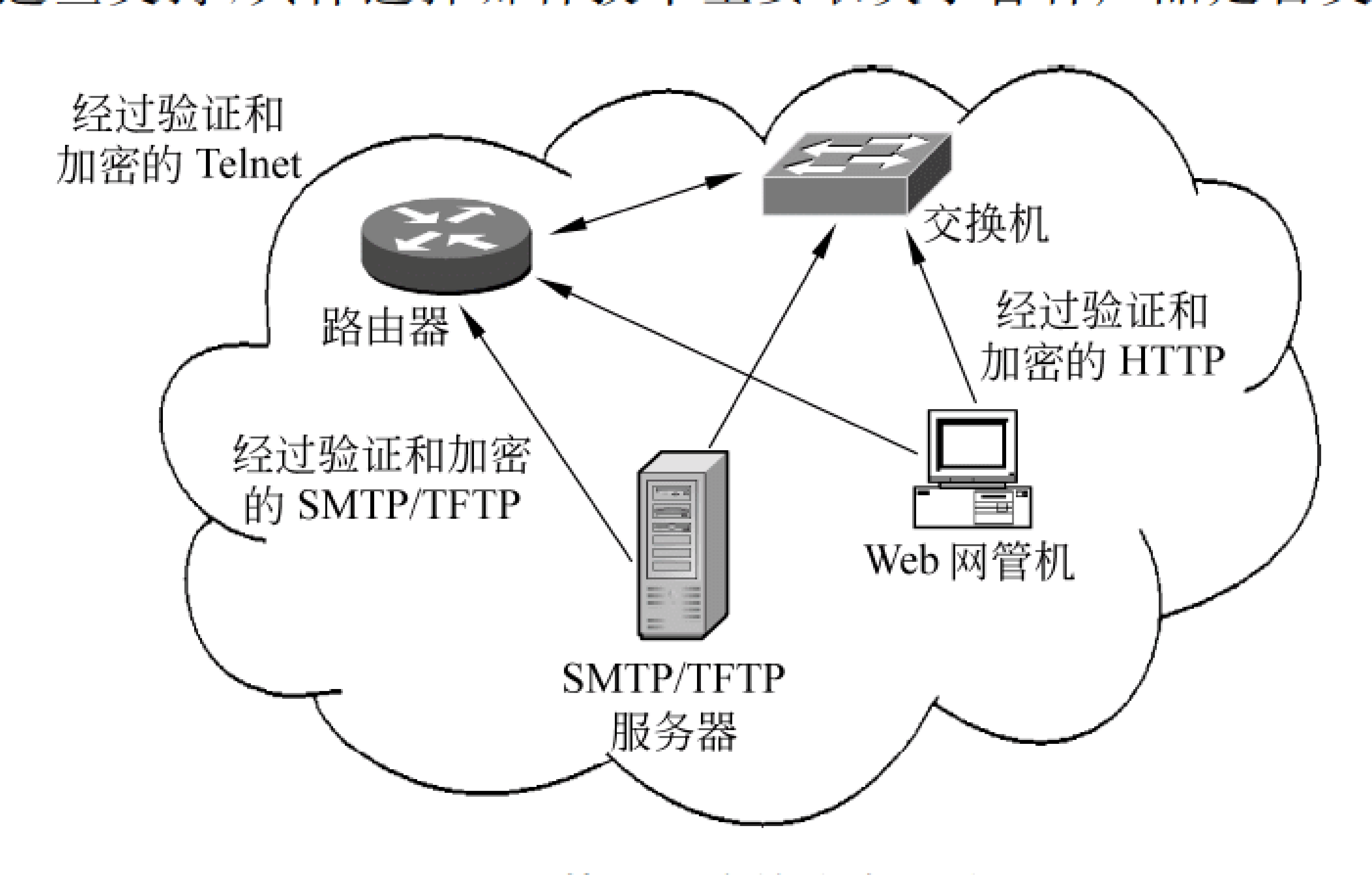



**图 3-2　基础设施的安全通信**

### 3.2.5 人员角色与行为规则

人员角色管理是整个网络安全的重要组成部分,网络中所有的软硬件系统、安全策略等最终都需要人来实践,所以对人员角色的定义及行为规则的制定是非常重要的。应当根据网络安全策略来为负责网络基础设施维护和升级的人员制定特殊的指导方针,以帮助完成各自的任务,这些任务主要包括安全备份和审计跟踪的工作等。

#### 1. 安全备份

创建备份的过程是运行计算机网络环境的一个完整部分，对于网络基础设施框架，提供网络应用服务的服务器的备份以及网络基础设施设备配置和映射的备份都是很重要的。备份策略包括确保用户已经对所有网络基础设施设备的配置和软件映射进行了备份，确保用户已经对所有提供网络服务的服务器进行了备份，确保用户的备份文件不被存储在同一个存储点上。管理员应该认真选择数据存储点，不但需要考虑其安全性和可用性，还需要考虑为备份文件加密，使备份信息一离开原点就得到额外的保护。需要注意的是，用户还应该有良好的密钥管理体制，这样才能够在需要时恢复数据。此外，还要确保在将来需要解密时能访问必要的解密程序。不要总是设想自己的备份是完好的，需要定期验证备份文件的正确性和完整性，并保持原件的数据、程序和备份的安全。将备份件与原件分开进行异地保存是一个十分重要的方法，这样做不仅考虑到了数据损害问题，同时还可以防止失窃。另外，用于记录和存储这些敏感软件或数据的介质，在不用时也应该加以识别与保护。

#### 2. 审计跟踪

对通信方式以及所有非法行为进行记录，以及对用户名、主机名、IP 源地址、目的地址端口号和时间戳进行记录，并对这些数据进行分析，有可能会发现安全被突破的第一条线索。管理员根据数据的重要性，可以将其保存在资源本地，直到它被需要或在每个事件后被转存为止。由于审计数据可能是站点上和备份文件中一些最需要认真保护的数据，如果入侵者能够侵入到审计记录，系统将会受到重要的安全威胁，所以有可能的话也需要将这些审计记录进行有效的备份。此外，审计数据也可以成为有法律效力的数据，成为跟踪入侵者以及证明其入侵行为的有效证据，所以对审计数据应小心谨慎处理，以避免因为没有适当处理而造成严重后果。

### 3.2.6 一个网络安全策略示例

通过上面讲述的有关网络安全策略的制定与实施，可以利用一个模拟的局域网络编写一个简单的安全策略作为例子，为了方便理解与讲述，仅做简单描述，更为详细与具体的内容没有列出。由于网络的重要性、应用和规模等都存在差异，安全策略并不是一成不变，用户必需根据实际情况，对安全策略进行必要的增添、删除与修改。

这是一个较小的局域网络，其拓扑结构如图 3-3 所示。

#### 1. 物理安全

(1) 所有建筑内的网络设备间必须按照相关的防火和安全标准构建。

(2) 所有设备间必须进行保护，安装防盗门，防止受到潜在的人为破坏或自然灾害损坏。

(3) 所有网络基础设备必须安装冗余电源，防止由于电源故障而引起网络中关键应用的中断。

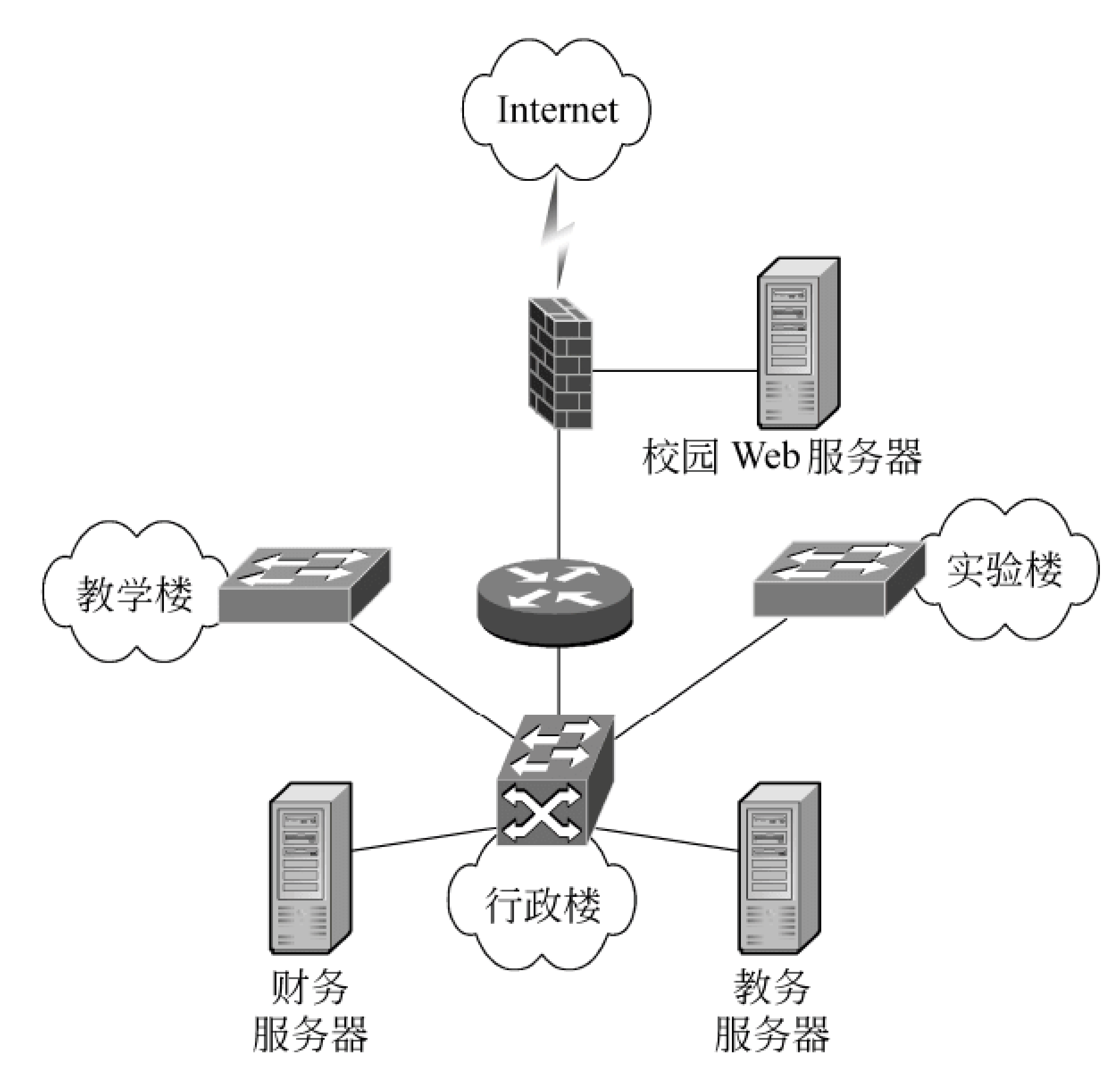



**图 3-3　一个校园拓扑示意图**

(4) 所有网络基础设备必须锁在设备柜里,只有维修人员可以打开访问,其他人无权访问。

## 2. 物理维护

(1) 只有网络设备维护小组的成员才有权访问设备间和设备机柜。

(2) 其他人员如有必要(如电源维修),必须在网络设备维护小组的成员陪同下打开设备间。

(3) 设备间必须安装远程监控系统。

(4) 当维护小组成员发生人事变动时,需更换设备间的锁。

## 3. 逻辑网络规划

(1) 所有外部人员需要访问的资源全部划分到防火墙的 DMZ 区上(如 WWW 服务)。

(2) 根据部门不同,将其他网络分隔成 VLAN,分别提供给行政、教学、财务和普通用户。

(3) 网络监控系统独立构成一个 VLAN,并不得与其他网段进行数据交换。

(4) 财务部门需建立一个独立的子网,不与外界数据进行通信。

(5) 所有基础设备和关键服务都位于各自的子网中。

## 4. 网络访问策略

(1) 普通用户只能访问外网。

(2) 只有财务有权访问财务子网。

(3) 行政人员有权访问除监控、财务外的其他子网。

### 5. 访问网络设备

(1) 只有网络设备维护组的成员才能通过 Telnet 方式访问网络基础设施设备。
(2) 对网络基础设施的访问采用一次性密码鉴别技术。
(3) 所有基础设备通常都有注册提示,提示的信息不应该包括系统类型或设备名称。
(4) 记录对基础设备执行的所有操作。

### 6. 基础设施安全性

(1) 如果交换机 LAN 端口和路由器接口没有被使用时,禁止对它们的访问。
(2) 防火墙的功能被作用在出口点和应用服务器子网前端。
(3) 只支持必要的网络服务,这些服务由网络安全指导小组来确定。

### 7. 数据完整性

(1) 在关键服务器与个人计算机中不得使用与工作无关的软件。
(2) 所有软件映射和操作系统在安装前都必需采用校验和确认机制来确认其完整性。
(3) 所有路由更新和 VLAN 更新信息都必需在发送和接收设备之间进行验证。

### 8. 数据保密性

(1) 所有学生成绩的信息必须加密。
(2) 所有关于财务的信息必须加密。
(3) 所有教工信息和利益的信息必须加密。

### 9. 个人安全控制

(1) 必须确定各应用系统关键职位的人选,确定可能的继任者。
(2) 新来的负责执行和操作网络基础设施设备的员工需要通过全面的背景材料调查。
(3) 所有涉及网络基础设备的人员,包括技术支持和管理人员都必须参加安全技术讲座。

### 10. 设备的采购与维护

(1) 所有基础设施设备在买进之前必须通过采购认证。
(2) 所有新的映射和配置在投入使用之前必须先在测试设备上经过模拟。
(3) 所有预定的主要网络停机和中断服务都需提前通知可能受到影响的部门。

### 11. 备份程序

(1) 所有软件映射和配置在修改前必须在基础设施设备上留有备份。
(2) 原来的映射和配置文件必须保留到进行另一次修改时。

（3）所有备份必须存储在专用的加锁的地方。

**12. 用户安全教育**

（1）每半年进行一次网络安全培训。
（2）不得使用盗版操作系统及相关软件。
（3）正常情况下，所有密码不得通过纸张、邮件、网络通信软件及电话传送。
（4）在交换密码等核心数据时，必需通过身份鉴别才能交换，并留下交换记录。
（5）用户离职，需及时删除其在各个应用系统中的权限。

## 3.3 网络安全测试工具的使用

在了解完安全策略的制定过程后，对网络现状的调查与了解，则是制定网络安全策略的必要前提。如果对网络的运行状况一无所知，或者知之甚少的话，根本无法制定出科学合理的安全策略。不是过于庞杂无法实施，就是毫无重点达不到预期效果。事实上，在网络攻击者对特定网络进行入侵过程中，第一步也是对目标网络进行侦测，以了解该网络的缺陷及薄弱环节，从而确定下一步的工作。所以，无论是网络的管理者和入侵者都需要掌握一些网络测试工具，利用这些工具来对整个网络的运行状况进行测试，以便了解网络现状，及时弥补一些显而易见的安全漏洞。从而加固网络系统，增加网络安全。下面就对一些常用的网络安全测试工具分别进行叙述。

### 3.3.1 扫描原理及其工具

面对网络越来越多的安全入侵，如果能够尽可能早地发现网络系统安全漏洞，并及时采取适当的处理措施进行修补，就可以有效地阻止入侵事件的发生。利用扫描工具对系统进行安全扫描，是了解目前网络运行情况的有效方法。通过扫描来了解系统向外界提供了哪些服务，或者探测目标主机系统端口目前正在向外提供何种服务。扫描技术利用 TCP/IP 协议标准和其在各种操作系统中不同的实现方式，向目标主机的服务端口发送探测数据包，并记录目标主机的响应。通过分析响应的数据包来判断服务端口是打开还是关闭，就可以得知端口提供的服务或信息。它可以搜集到目标主机的各种信息，如是否能用匿名登录，是否有可写的 FTP 目录，是否能用 Telnet 等。扫描也可以通过捕获本地主机或服务器的流入流出数据包来监视本地 IP 主机的运行情况，它能对接收到的数据进行分析，帮助人们发现目标主机的某些内在弱点。扫描工作本身不会提供侵入一个系统的详细方法，只是系统入侵的前奏。系统扫描通常采用两种策略，第一种是被动式策略，第二种是主动式策略。所谓被动式策略就是基于主机之上，对系统中不合适的设置、脆弱的密码以及其他同安全规则抵触的对象进行检查；而主动式策略是基于网络的，它通过执行一些脚本文件模拟对系统进行攻击的行为并记录系统的反应，从而发现其中的漏洞。

扫描软件从最初专门为 UNIX 系统编写的一些只具有简单功能的小程序，发展到现在已经出现了多个运行在各种操作系统平台上的、具有复杂功能的商业程序。这些软件

常用的有如下几种实现方式。

(1) 使用插件。每个插件都封装有一个或者多个漏洞的测试手段,主扫描程序通过调用插件的方法来执行扫描。添加新的插件就可以使软件增加新功能,用来扫描更多的漏洞。在插件编写规范公布的情况下,用户或者第三方公司甚至可以自己编写插件来扩充软件的功能。这种技术使软件的升级维护都变得相对简单,并具有非常强的扩展性。

(2) 使用专用脚本语言。事实上这是一种更高级的插件技术,用户可以使用专用脚本语言来扩充软件功能。脚本语言的使用简化了编写新插件的编程工作,使扩充软件功能的工作变得更加容易和方便。

(3) 安全评估专家系统。现在较成熟的扫描系统都能够将对主机的扫描结果进行整理并形成报表,能够对一些具体漏洞提供相应的解决方法,并能对网络的状况形成一个整体的评估。而不是像一些较早的漏洞扫描程序只是简单地把各个扫描测试项的执行结果罗列出来,不对信息进行任何分析处理直接提供给测试者。从扫描系统发展的规律来看,未来的安全扫描系统不但能够扫描安全漏洞,还能够智能化的协助网络信息系统管理人员评估本网络的安全状况给出安全建议,成为一个安全评估专家系统。

目前常用的专业扫描工具有 SuperScan、nmap、Nessus、ShadowScan 等,其中有些只能在 Windows 系统下运行,有的只能在 BSD 系统下运行。它们都是广为流传、应用广泛的扫描工具,是攻击者与被攻击者都可以得到的强大的信息收集工具。在执行扫描工作的时候,由于其对系统有一定的影响,所以必须要考虑到网络的承受能力和对目标计算机的影响。同时,无论是出于某种目的,扫描工作必须在国家法律法规允许的范围进行。由于扫描工具很多,本书仅选取在 Windows 系统和 BSD 系统下常见的 SuperScan 和 nmap 进行重点介绍。

**1. SuperScan 的使用**

SuperScan 是一款在 Windows 下使用较多专业扫描软件,由 Foundstone 公司出品,目前较新的版本是 SuperScan 4.0。它是一款免费的扫描软件,用户下载后无须安装,直接可以运行使用。它能够通过 ping 命令来检验 IP 是否在线,可以进行 IP 和域名相互转换,能够检验目标计算机提供的服务类别,检验一定范围内目标计算机是否在线和端口情况,还可以使用工具自定义列表检验目标计算机,也可以自定义要检验的端口,并保存为端口列表文件。它还自带一个木马端口列表 trojans.lst,通过这个列表可以检测目标计算机是否有木马。同时,也可以自己定义修改这个木马端口列表。可以看出,这款软件几乎将与 IP 扫描有关的所有功能全部做到了,而且每一个功能都很专业。

1) 软件具体使用

SuperScan 4.0 是免费的扫描软件,可以在 http://www.foundstone.com 网站上下载,是一个 196kb 的 Zip 压缩包。因为 SuperScan 运行时有可能引起网络包溢出,所以 Foundstone 网站声明某些杀毒软件可能识别 SuperScan 是一款拒绝服务攻击(DoS)的代理,需要关闭杀毒软件才能正常运行。此软件是一款绿色软件,无须进行系统安装,下载后直接运行就可以工作了。运行程序时,出现程序运行窗口,如图 3-4 所示。

SuperScan 软件使用非常简便,其主要功能有扫描、主机与服务发现、扫描选择、工

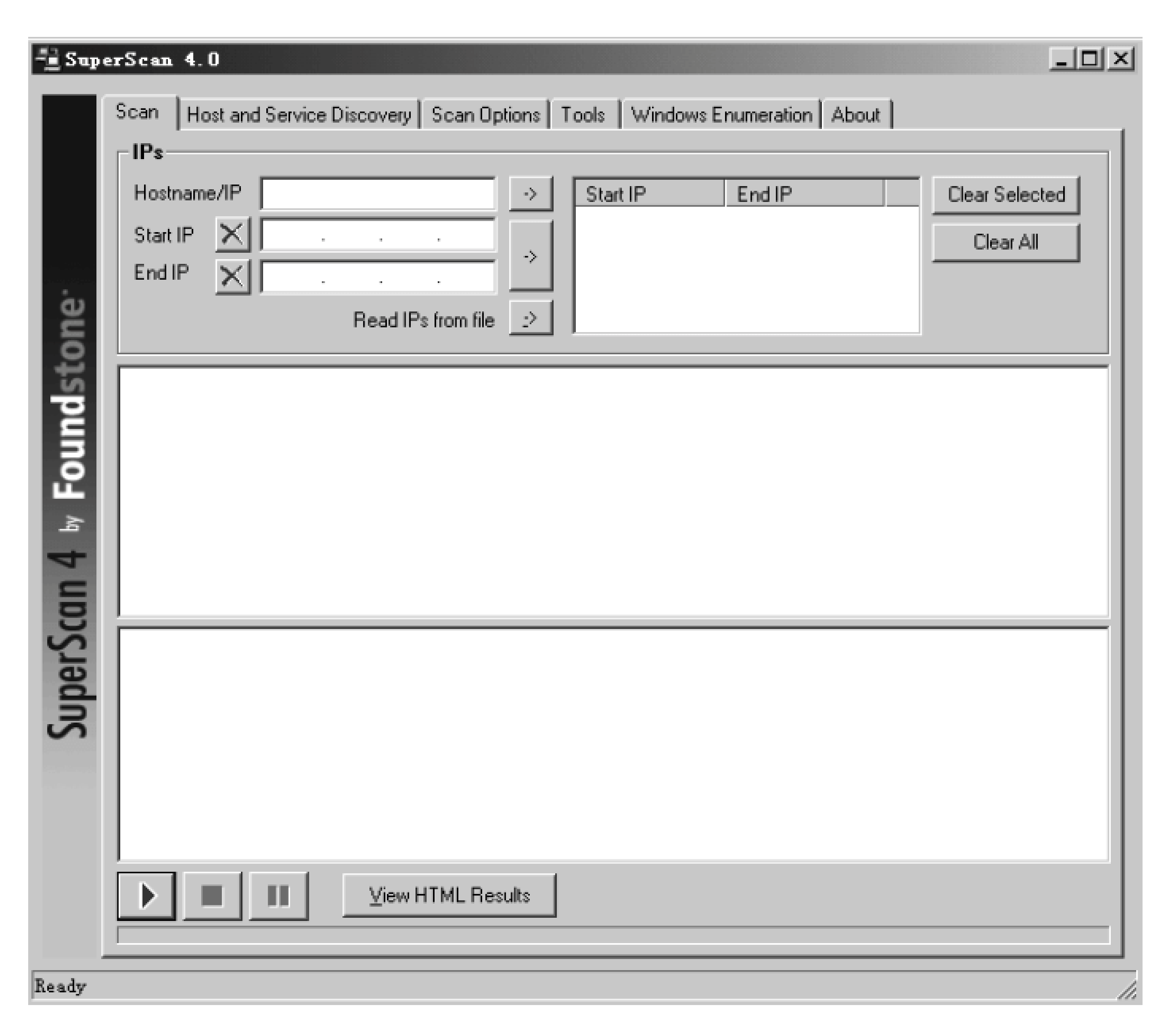



图 3-4 SuperScan 4.0 运行的主界面

具、窗口列举等。

2）扫描

SuperScan 扫描包括主机扫描以及对地址段的扫描。在 Hostname/IP 后输入域名，系统会自动将 IP 地址解析出来，如图 3-5 所示。SuperScan 允许输入要扫描的 IP 范围，进行整个网段的快速扫描。

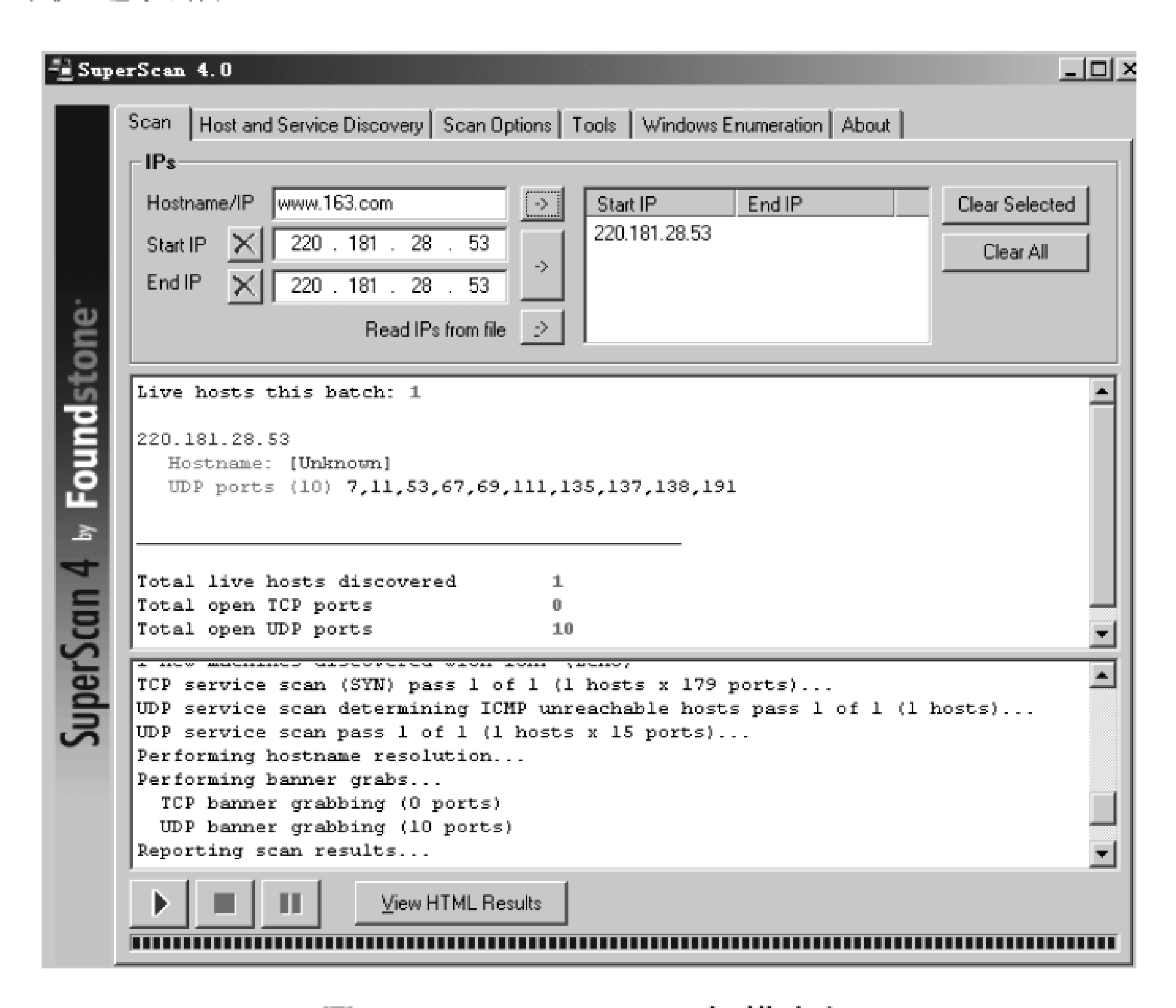



图 3-5 SuperScan 4.0 扫描主机

按下扫描按钮后，系统开始对地址(段)进行扫描。扫描进程结束后，SuperScan 将提供一个主机列表，列出关于每台扫描过的主机被发现的开放端口信息。SuperScan 可以将扫描了哪些主机和在每台主机上哪些端口是开放的结果以 HTML 文件格式显示出来，如图 3-6 所示。

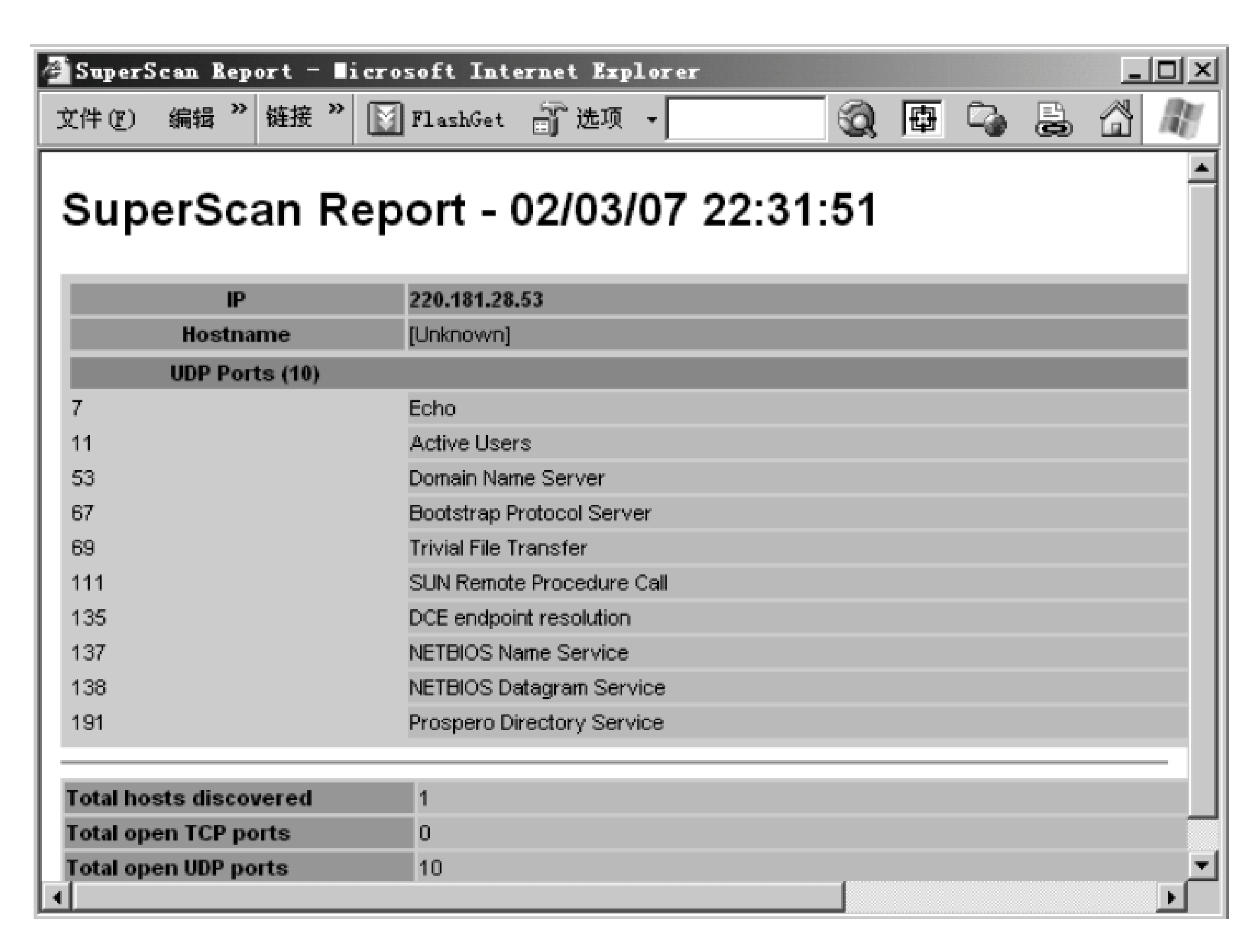



图 3-6　HTML 格式显示结果

3) 关于主机和服务器扫描设置

通过一些初步设置，已经能够从一群主机中执行简单的扫描，然而很多时候需要定制扫描。这时，要用到 Host and Service Discovery 选项卡，如图 3-7 所示。利用这个选

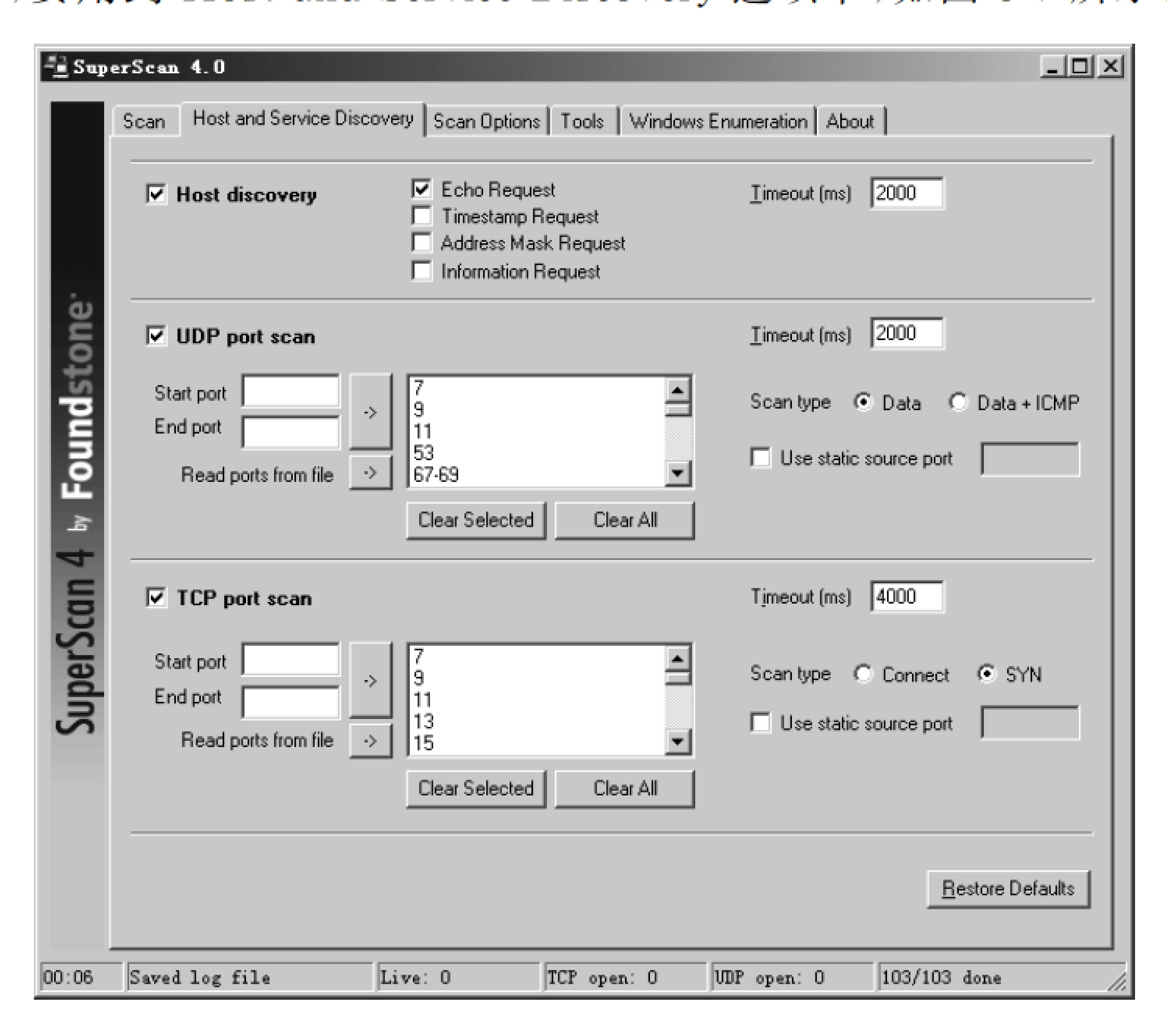



图 3-7　Host and Service Discovery 选项卡

项,可以让用户在扫描的时候看到更多信息。它包括主机发现选项(host discovery)和UDP端口扫描及TCP端口扫描。

发现主机的方法是通过重复请求(echo requests)来实现,也可以通过时间戳请求(timestamp)、地址屏蔽请求(address mask requests)和消息请求(information requests)来发现主机。SuperScan最初开始扫描的仅仅是那几个最常用的端口,主要的原因是因为有超过65000个的TCP和UDP端口,若对每个可能开放端口的IP地址进行超过130000次的端口扫描,那将需要很长的时间。因此,SuperScan最初开始扫描的只是几个最常用的端口,但也提供给用户扫描额外端口的选项。

如果检测的时候没有特定的目的,只是为了了解目标计算机的一些情况,可以对目标计算机的所有端口进行检测。需要注意的是选择的选项越多,那么扫描用的时间就越长。它会对目标计算机的正常运行造成一定影响,同时也会引起目标计算机的警觉,还会浪费带宽资源,对网络正常运行造成影响。如果用户正在试图尽量多的收集一个明确的主机信息,建议首先执行一次常规的扫描以发现主机,然后再利用可选的请求选项来扫描。

其实,大多数时候不需要检测所有端口,只要检测有限的几个端口就可以了,因为目的只是为了得到目标计算机提供的服务和使用的软件。所以,可以根据不同的目的来检测不同的端口,大部分时候只要检测80(Web服务)、21(FTP服务)、23(Telnet服务)等常用的端口就可以了。即使是攻击性检测,也不会有太多的端口需要扫描。使用自定义端口的方式有以下优点。

(1) 选择端口时可以详细了解端口信息。

(2) 选择的端口可以自己取名保存,有利于再次使用。

(3) 可以要求工具有的放矢的检测目标端口,节省时间和资源。

(4) 根据一些特定端口,可以检测目标计算机是否被攻击者利用、种植木马或打开不应该打开的服务。

4) 扫描选项(Scan Options)

如图3-8所示,Scan Options选项允许进一步的控制扫描进程,能够控制扫描速度和通过扫描的数量。菜单中的首选项是定制扫描过程中主机和通过审查的服务数。默认值是1,一般来说足够了,除非网络连接不太可靠时才要进行修改。

Scan Options中的另一个选项是设置主机名解析的数量。同样,使用默认值1足够了,除非在连接不可靠时要进行更改。另一个选项是获取标志(banner grabbing)的设置,Banner Grabbing是根据显示一些信息尝试得到远程主机的回应。默认的延迟是8000ms,如果所连接的主机比较慢,这个时间就不太够。旁边的滚动条是扫描速度调节选项,利用它能调节SuperScan发送每个包所要等待的时间。扫描最快的是调节滚动条将其设为0。但是当扫描速度设置为0时,则存在包溢出的潜在可能。如果担心由于SuperScan引起的过量包溢出,最好调慢SuperScan的速度。

5) 工具(Tools)选项

SuperScan的工具选项(Tools)是非常有用的选项,它集成了许多工具集。这些工具集包括DNS解析、ping工具和Traceroute工具等常用的网络测试工具。通过利用这些

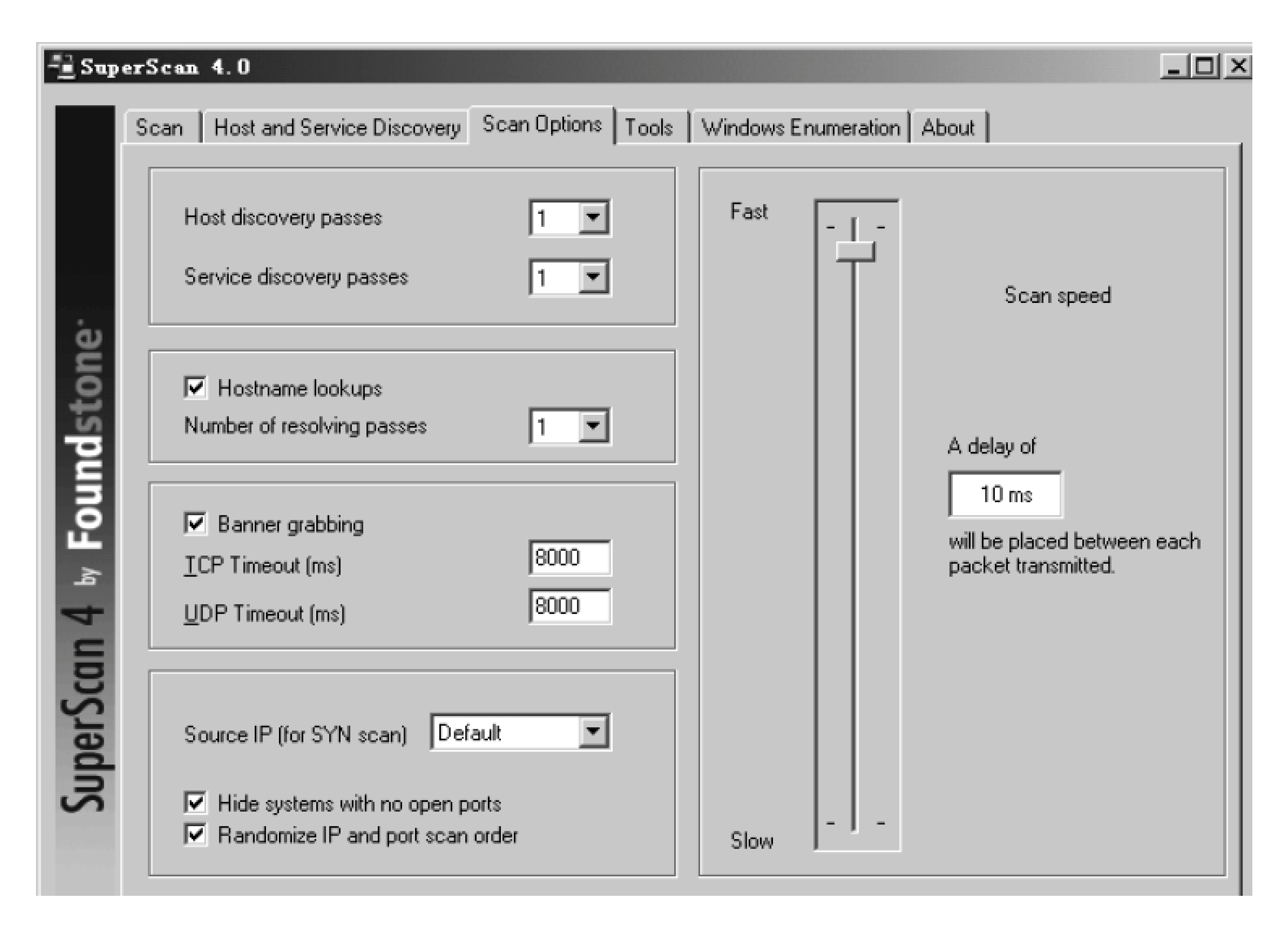



图 3-8　Scan Options 选项卡

工具可以使用户很快的得到许多关于指定主机的信息。正确输入主机名或 IP 地址和默认的连接服务器，然后单击要得到信息的相关按钮。如可以试着 ping 一台服务器或 Traceroute 和发送一个 HTTP 请求。图 3-9 显示了得到的各种信息。

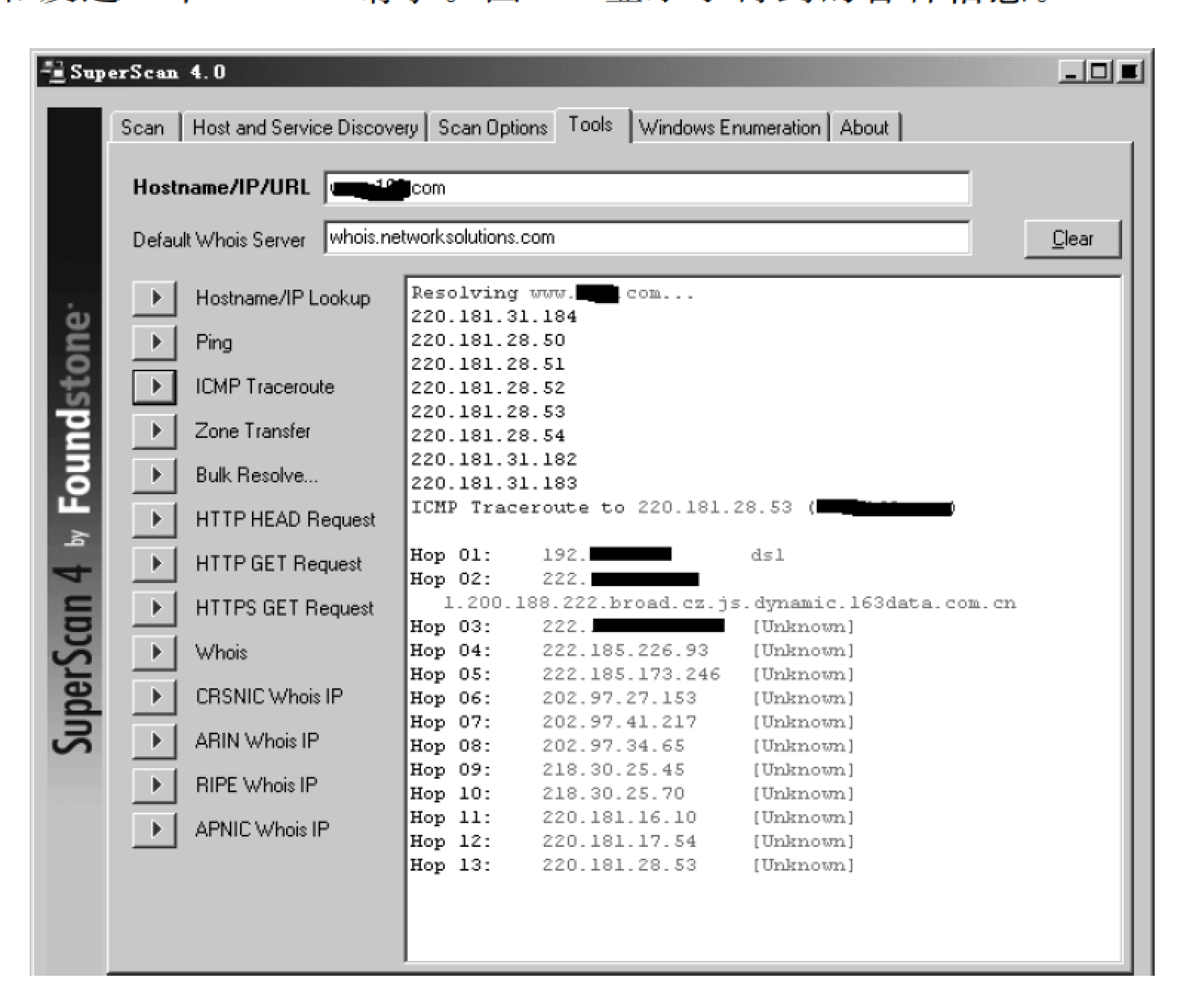



图 3-9　通过不同的按钮收集主机信息

6) Windows 枚举选项(Windows Enumeration)

最后一个功能选项是 Windows 枚举选项，如果用户设法收集信息的是 Linux/UNIX 主机，那这个选项是没什么用的。但如果需要 Windows 主机的信息，它确实是很方便

的。如图 3-10 所示，它能够提供从单个主机到用户群组，再到协议策略的所有信息。这个选项给人最深刻的印象是它产生的大量透明信息。

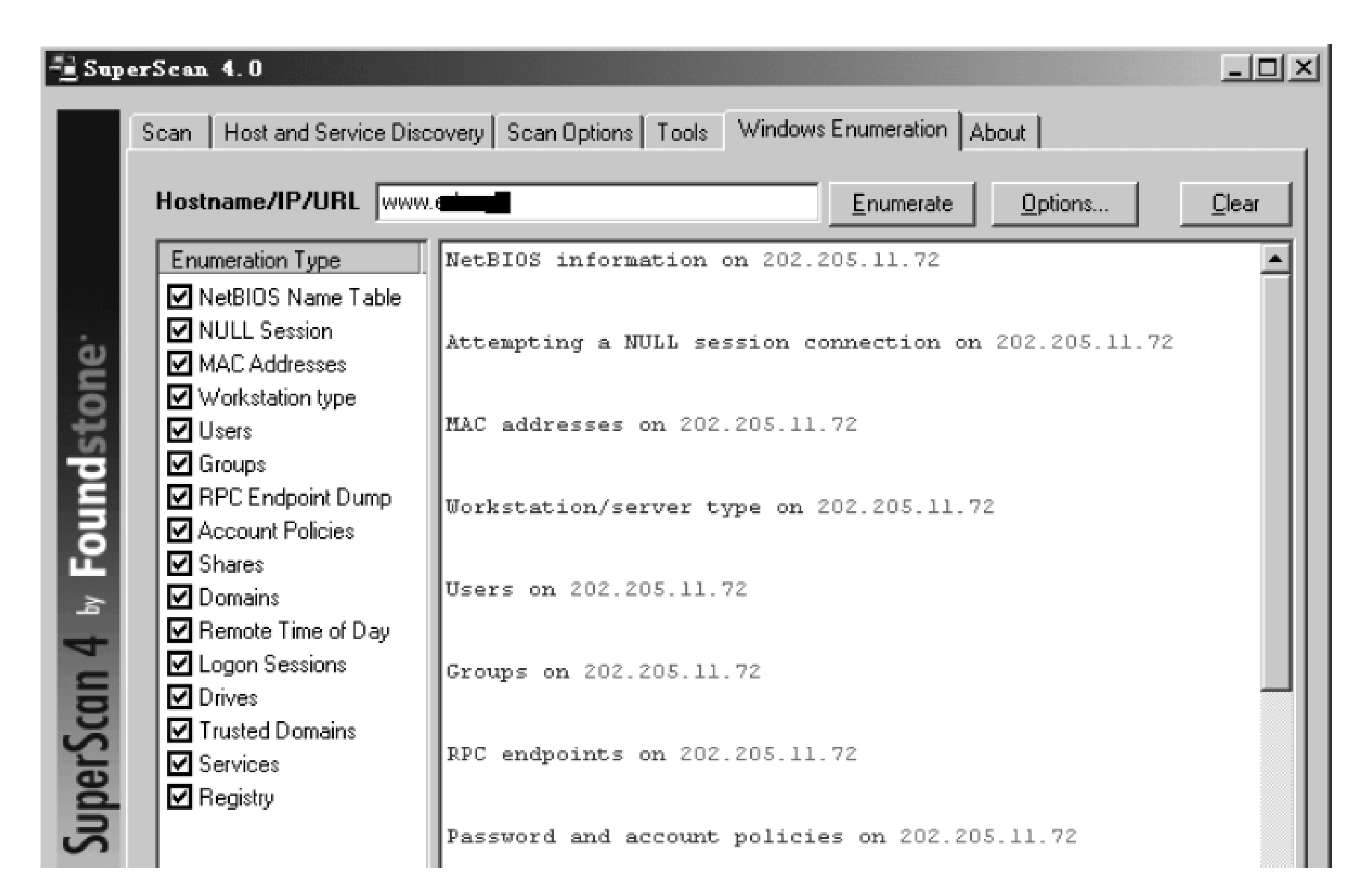



**图 3-10 Windows 枚举选项能够产生关于 Windows 主机的大量信息**

SuperScan 是系统管理员常备的几种工具之一。可将其作为日常安全审核工具包的一部分。如果管理员知道入侵者能够看到自己所管理的网络中的哪些信息，那么就有可能采取相应的措施，减少潜在攻击，有效地保护网络系统。

### 2. nmap 的使用方法

nmap 是一个强大的、传统的网络检测和安全扫描程序，它最初是在 UNIX 环境下运行的。它在各类 BSD 系统内都有着很好的表现，目前已经移植到 Windows 平台了。用户可以通过这个软件来对大型网络进行扫描获取需要的信息，如主机正在运行什么操作系统，提供了什么服务等。nmap 是一个极为强大的工具，其综合了多种扫描模式，如 UDP、TCP Connect、TCP SYN、FTP 代理、ICMP、FIN、ACK 扫描、SYN 扫描、null 扫描等。同时还提供了一些高级的特征，如通过 TCP/IP 协议栈特征探测操作系统类型、秘密扫描、动态延时和重传计算、并行扫描、通过并行 ping 扫描探测关闭的主机、诱饵扫描、避开端口过滤检测、直接 RPC 扫描、碎片扫描以及灵活的目标及端口设定。

nmap 扫描主机后，一般会列出端口的列表，给出端口的服务名、端口号、状态和协议等信息，如下所示。

```
[root@ test root]#nmap 127.0.0.1
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on   (192.168.0.1):
(The 1582 ports scanned but not shown below are in state: closed)
Port        State       Service
80/tcp      open        http
135/tcp     filtered    loc-srv
161/tcp     filtered    snmp
```

```
445/tcp     filtered    microsoft-ds
777/tcp     filtered    unknown
5900/tcp    filtered    vnc
Nmap run completed -- 1 IP address (1 host up) scanned in 38 seconds
```

每个端口的状态有 open、filtered、unfiltered 三种形式。open 状态意味着目标主机能够在这个端口使用 accept()系统调用接受连接。filtered 状态表示被防火墙、包过滤或其他的安全软件掩盖了这个端口，禁止 nmap 探测其是否打开。unfiltered 表示这个端口关闭，并且没有防火墙/包过滤软件来隔离 nmap 的探测企图。通常情况下，端口的状态基本都是 unfiltered 状态，只有在大多数被扫描的端口处于 filtered 状态下，才会显示处于 unfiltered 状态的端口。根据使用的功能选项，nmap 也可以报告远程主机所使用的操作系统、TCP 序列、运行绑定到每个端口上的应用程序的用户名、DNS 名、主机地址是否是欺骗地址以及其他一些东西。在 Linux/UNIX 下运行的 nmap 一般只能由 root 用户使用。通常 Linux 系统会将 namp 预装在系统内，无须进行安装直接使用就可以了。可以使用下面的命令来查看所使用的 nmap 版本。

```
[root@ test root] nmap - version
```

如果系统内存在 nmap 的话，会显示 nmap 的版本号。如果系统中没有预装的话，可以到 http://insecure.org/nmap/download.html 上去下载最新版本的 nmap 程序。由于 nmap 更新较快，但其基本的用法一样，我们以 nmap 4.2 版本为例，在 Linux 系统下详细说明其使用方法，nmap 的功能选项可以组合使用，一些功能选项只能够在某种扫描模式下使用。nmap 会自动识别无效或者不支持的功能选项组合，并向用户发出警告信息。可以使用下面的命令来快速列出功能选项的列表。

```
[root@ test root]#nmap - h
```

1）功能参数选项

（1）参数：-sS

TCP 同步扫描(TCP SYN)因为不必全部打开一个 TCP 连接，所以这项技术通常称为半开扫描(half-open)。可以发出一个 TCP 同步包(SYN)，然后等待回应。如果对方返回 SYN/ACK(响应)包就表示目标端口正在监听；如果返回 RST 数据包，就表示目标端口没有监听程序。如果收到一个 SYN/ACK 包，源主机就会马上发出一个 RST(复位)数据包断开和目标主机的连接，它实际上由操作系统内核自动完成的。这项技术最大的好处是很少有系统能够把这记入系统日志，不过需要 root 权限来定制 SYN 数据包。

（2）参数：-sT

这是最基本的 TCP 扫描方式。connect()是一种由操作系统提供的系统调用，用来打开一个链接。如果目标端口有程序监听，connect()就会成功返回，否则这个端口是不可达的。其最大的优点是任何 UNIX 用户都可以自由使用这个系统调用。这种扫描很容易被检测到，在目标主机的日志中会记录大批的连接请求以及错误信息。

（3）参数：-sU

UDP 扫描。如果想知道在某台主机上提供哪些 UDP(用户数据报协议，RFC768)服

务，可以使用这种扫描方法。nmap 首先向目标主机的每个端口发出一个 0 字节的 UDP 包，如果收到端口不可达的 ICMP 消息，端口就是关闭的；否则就假设它是打开的。

(4) 参数：-sP

这是 ping 扫描。有时候只是想知道此时网络上哪些主机正在运行。通过向指定网络内的每个 IP 地址发送 ICMP echo 请求数据包，nmap 就可以完成这项任务。如果主机正在运行就会作出响应。不幸的是，一些站点会阻塞 ICMP echo 请求数据包。然而，在默认的情况下 nmap 也能够向 80 端口发送 TCP ack 包，如果收到一个 RST 包，就表示主机正在运行。nmap 使用的第三种技术是发送一个 SYN 包，然后等待一个 RST 或者 SYN/ACK 包。对于非 root 用户，nmap 使用 connect()方法。在默认的情况下(root 用户)，nmap 并行使用 ICMP 和 ACK 技术。注意，nmap 在任何情况下都会进行 ping 扫描，只有目标主机处于运行状态，才会进行后续的扫描。如果只是想知道目标主机是否运行，而不想进行其他扫描，才会用到这个选项。

(5) 参数：-sF -sX -sN

这是秘密 FIN 数据包扫描、圣诞树(Xmas Tree)、空(Null)扫描模式，在 SYN 扫描都无法确定的情况下使用。一些防火墙和包过滤软件能够对发送到被限制端口的 SYN 数据包进行监视，而且有些程序(如 synlogger 和 courtney)能够检测哪些扫描。这些高级的扫描方式可以逃过这些干扰，理论依据是关闭的端口需要对探测包回应 RST 包，而打开的端口必须忽略有问题的包。FIN 扫描使用暴露的 FIN 数据包来探测，而圣诞树扫描打开数据包的 FIN、URG 和 PUSH 标志。由于微软的操作系统忽略这个标准，所以这种扫描方式对 Windows 系统无效。

(6) 参数：-sA

ACK 扫描。这项高级的扫描方法通常用来穿过防火墙的规则集。通常情况下，这有助于确定一个防火墙是功能比较完善的还是一个简单的包过滤程序只是阻塞进入的 SYN 包。这种扫描是向特定的端口发送 ACK 包(使用随机的应答/序列号)。如果返回一个 RST 包，这个端口就标记为 unfiltered 状态。如果什么都没有返回或返回一个不可达 ICMP 消息，这个端口就归入 filtered 类。注意，nmap 通常不输出 unfiltered 的端口，所以在输出中通常不显示所有被探测的端口，显然这种扫描方式不能找出处于打开状态的端口。

(7) 参数：-sW

对滑动窗口的扫描。这项高级扫描技术非常类似于 ACK 扫描，它有时可以检测到处于打开状态的端口。因为滑动窗口的大小是不规则的，有些操作系统可以报告其大小。这些系统包括某些版本的 AIX、OpenBSD、SunOS 4.x、Ultrix 等。

(8) 参数：-sR

这是 RPC 扫描。这种方法要和 nmap 的其他端口扫描方法结合使用。选择所有处于打开状态的端口向它们发出 SunRPC 程序的 NULL 命令，以确定它们是否是 RPC 端口。如果是，就确定是哪种软件及其版本号。因此能够获得防火墙的一些信息。但诱饵扫描现在还不能和 RPC 扫描结合使用。

(9) 参数：-sL

列出扫描结果。这个方法不需要真正的 ping 或扫描主机，能简单执行并打印出 IPs/Name 列表。DNS 名称解析将被执行，除非使用了-n 参数。

(10) 参数：-b

FTP 反弹攻击(bounce attack)。FTP 协议支持代理 FTP 连接。也就是说，能够从 source.com 连接到 FTP 服务器 target.com，并且可以要求这台 FTP 服务器为自己发送 Internet 上任何地方的文件。可以使用这个特征，让一台代理 FTP 服务器扫描 TCP 端口，需要先连接到防火墙后面的一台 FTP 服务器，接着进行端口扫描。如果在这台 FTP 服务器中有可读写的目录，还可以向目标端口任意发送数据。传递给功能选项-b 参数的是要作为代理的 FTP 服务器。语法格式为。

```
-b username:password@server:port
```

除了 server 以外，其余都是可选的。

2) 通用选项

(1) 参数：-P0

在扫描之前，不必 ping 主机。因为有些网络的防火墙不允许 ICMP echo 请求穿过，使用这个选项可以对这些网络进行扫描。

(2) 参数：-PT

扫描前，使用 TCP ping 确定哪些主机正在运行。注意 nmap 并不是通过发送 ICMP echo 请求包，然后等待响应来实现这种功能，而是向目标网络(或者单一主机)发出 TCP ACK 包然后等待回应。如果主机正在运行就会返回 RST 包。只有在目标网络/主机阻塞了 ping 包，而仍旧允许对其进行扫描时，这个选项才有效。对于非 root 用户，可以使用 connect()系统调用来实现这项功能。使用-PT ＜端口号＞来设定目标端口，由于 80 端口常被用来提供 Web 服务，通常不会被过滤，所以被设定为默认端口号。

(3) 参数：-PS

对于 root 用户，这个选项让 nmap 使用 SYN 包而不是 ACK 包来对目标主机进行扫描。如果主机正在运行就返回一个 RST 包；否则返回一个 SYN/ACK 包。

(4) 参数：-PI

设置这个选项，让 nmap 使用真正的 ping(ICMP echo 请求)来扫描目标主机是否正在运行。使用这个选项让 nmap 发现正在运行的主机的同时，nmap 也会对直接子网广播地址进行观察。直接子网广播地址是一些外部可达的 IP 地址，把外部的包转换为一个内向的 IP 广播包，向一个计算机子网发送。这些 IP 广播包应该删除，因为会造成拒绝服务攻击(如 smurf)。

(5) 参数：-PP

使用一个 ICMP 的时间戳请求包来发现主机。

(6) 参数：-PM

用法与 -PI 和-PP 相类似，除了需要使用掩码。

(7) 参数：-PB

这是默认的 ping 扫描选项。它使用 ACK(-PT)和 ICMP(-PI)两种扫描类型并行扫描。如果防火墙能够过滤其中一种包,使用这种方法就能够穿过防火墙。

(8) 参数:-O

这个选项激活对 TCP/IP 指纹特征(fingerprinting)的扫描,获得远程主机的标志。也就是说 nmap 使用一些技术来检测目标主机操作系统网络协议栈的特征。nmap 使用这些信息建立远程主机的指纹特征,把它和已知的操作系统指纹特征数据库做比较,就可以知道目标主机操作系统的类型。

(9) 参数:-I

这个选项打开 nmap 的反向标志扫描功能。ident 协议(rfc 1413)允许使用 TCP 连接给出任何进程拥有者的用户名,即使这个进程并没有初始化连接。例如,可以连接到 HTTP 端口,接着使用 identd 确定这个服务器是否由 root 用户运行。这种扫描只能在同目标端口建立完全的 TCP 连接时(例如,-sT 扫描选项)才能成功。使用-I 选项时,远程主机的 identd 守护进程就会查询在每个打开的端口上监听的进程的拥有者。如果远程主机没有运行 identd 程序,则这种扫描方法无效。

(10) 参数:-f

这个选项使 nmap 使用碎片 IP 数据包发送 SYN、FIN 和 NULL。使用碎片数据包会增加包过滤、入侵检测系统的难度,使其无法知道入侵企图。不过需要慎重使用这个选项,有些程序在处理这些碎片包时会有麻烦,在 nmap 中使用了 24 个字节的碎片数据包。虽然包过滤器和防火墙不能防止这种方法,但是有很多网络出于性能上的考虑,禁止数据包的分片。注意这个选项不能在所有的平台上使用,它在 Linux、FreeBSD、OpenBSD 以及其他一些 UNIX 系统能够很好工作。

(11) 参数:-v

冗余模式。使用这个选项,它会给出扫描过程中的详细信息。使用这个选项,可以得到事半功倍的效果。使用-d 选项可以得到更加详细的信息。

(12) 参数:-h

快速参考选项,用于列出主要的参数选项。

(13) 参数:-oN

把扫描结果重定向到一个可读的文件 logfilename 中。

(14) 参数:-oX

这个选项将扫描结果以 XML 的方式保存到文件中。

(15) 参数:-oG

这个选项将扫描结果以图形的方式保存到文件中。

(16) 参数:-oM

把扫描结果重定向到 logfilename 文件中,这个文件使用主机可以解析的语法。可以使用-oM -来代替 logfilename,这样输出就被重定向到标准输出 stdout。在这种情况下,正常的输出将被覆盖,错误信息仍然可以输出到标准错误 stderr。要注意,如果同时使用了-v 选项,在屏幕上会打印出其他的信息。

(17) 参数:-append_output

这个选项让 nmap 把扫描的结果附加到输出文件的内容后面，而不是将原来的内容覆盖。

（18）参数：-resume

某个网络扫描可能由于 control-C 或者网络损失等原因被中断，使用这个选项可以使扫描接着以前的扫描进行。logfilename 是被取消扫描的日志文件，它必须是可读形式或者机器可以解析的形式。而且接着进行的扫描不能增加新的选项，只能使用与被中断的扫描相同的选项。nmap 会接着日志文件中的最后一次成功扫描进行新的扫描。

（19）参数：-iL

从 inputfilename 文件中读取扫描的目标。在这个文件中要有一个主机或者网络的列表，由空格键、制表键或回车键作为分割符。如果使用-iL -，nmap 就会从标准输入 stdin 读取主机名字。可以从指定目标一节得到更加详细的信息。

（20）参数：-iR

让 nmap 自己随机挑选主机进行扫描。这个对于抽样统计网络来评估不同的情况很有用，如果真的厌倦使用，试着用 nmap -sS -iR -p 80 去发现一些 Web 服务器来测试一下。

（21）参数：-p ＜端口范围＞

这个选项要选择进行扫描的端口号范围。例如，-p 23 表示只扫描目标主机的 23 号端口。-p 20-30，139，60000-表示扫描 20 到 30 号端口、139 号端口以及所有大于 60000 的端口。在默认情况下，nmap 扫描从 1 到 1024 号以及 nmap-services 文件（如果使用 RPM 软件包，一般在/usr/share/nmap/目录中）中定义的端口列表。

（22）参数：-F

快速扫描模式，只扫描在 nmap-services 文件中列出的端口，显然比扫描所有 65535 个端口要快。

（23）参数：-D

使用诱饵扫描方法对目标网络/主机进行扫描。如果 nmap 使用这种方法对目标网络进行扫描，那么从目标主机/网络的角度来看，扫描就像从其他主机发出的。即使目标主机的 IDS（入侵检测系统）对端口扫描发出报警，它们也不可能知道哪个是真正发起扫描的地址，哪个是无辜的。这种扫描方法可以有效地对付如路由跟踪、response-dropping 等积极的防御机制，能够很好地隐藏 IP 地址。每个诱饵主机名使用逗号分割开，也可以使用 ME 选项，它代表自己的主机，和诱饵主机名混杂在一起。如果把 ME 放在第六或者更靠后的位置，一些端口扫描检测软件几乎不会显示扫描者的 IP 地址。如果不使用 ME 选项，nmap 会把你的 IP 地址随机夹杂在诱饵主机之中。用来作为诱饵的主机应该正在运行或只是偶尔向目标发送 SYN 数据包。很显然，如果在网络上只有一台主机运行，目标很轻松地就会确定是哪台主机进行的扫描。或许，还要直接使用诱饵的 IP 地址而不是其域名，这样诱饵网络的域名服务器的日志上就不会留下关于扫描者的记录。一些端口扫描检测软件会拒绝路由试图进行端口扫描的主机。如果这样，需要让目标主机和一些诱饵断开链接。如果诱饵是目标主机的网关或就是其自己时，会给目标主机造成很大问题。所以需要慎重使用这个选项。诱饵扫描既可以在起始的 ping 扫描也可以在

真正的扫描状态下使用。它也可以和-O 选项组合使用。使用太多的诱饵扫描能够减缓扫描速度甚至可能造成扫描结果不正确。同时,有些 ISP 会把欺骗包过滤掉,虽然现在大多数的 ISP 不会对此进行限制。

(24) 参数:-S <IP_Address>

在一些情况下,nmap 可能无法确定源地址(nmap 会通知)。在这种情况下,可以使用这个选项给出扫描者的 IP 地址。在欺骗扫描时,也使用这个选项,使用这个选项可以让目标认为是其他的主机对自己进行扫描。

(25) 参数:-e <interface>

告诉 nmap 使用哪个接口发送和接受数据包。nmap 能够自动对此接口进行检测,如果无效就会通知。

(26) 参数:-g <portnumber>

设置扫描的源端口。一些防火墙和包过滤器的规则集允许源端口为 DNS(53)或 FTP-DATA(20)的包通过和实现连接。显然,如果攻击者把源端口修改为 20 或 53,就可以摧毁防火墙的防护。在使用 UDP 扫描时,先使用 53 号端口。使用 TCP 扫描时,先使用 20 号端口。注意只有在能够使用这个端口进行扫描时,nmap 才会使用这个端口。如果无法进行 TCP 扫描,nmap 会自动改变源端口,即使使用了-g 选项。

(27) 参数:-n

告诉 nmap 不要对扫描到的地址进行反向解析 DNS,这可以加快扫描速度。

(28) 参数:-R

告诉 nmap 总是要对扫描到的目标地址进行反向解析。正常情况下,这个只在目标主机运行时起作用。

(29) 参数:-r

告诉 nmap 不要打乱被扫描端口的顺序。

(30) 参数:--randomize_hosts

使 nmap 在扫描之前,打乱每组扫描中的主机顺序,nmap 每组可以扫描最多 2048 台主机。这样,可以使扫描更不容易被网络监视器发现,尤其和--scan_delay 选项组合使用,更能有效避免被发现。

(31) 参数:-M

设置进行 TCP connect()扫描时,最多使用多少个套接字进行并行的扫描。使用这个选项可以降低扫描速度,避免远程目标宕机。

3) 适时选项

通常,nmap 在运行时,能够很好地根据网络特点进行调整。扫描时,nmap 会尽量减少被扫描目标检测到的机会,同时尽可能加快扫描速度。然而,nmap 默认的适时策略有时候不太适合所扫描的目标。使用下面这些选项,可以控制 nmap 的扫描时间。

(1) 参数:-T

设置 nmap 的适时策略。主要的模式包括:Paranoid,为了避开 IDS 的检测使扫描速度变得极慢,nmap 串行所有的扫描,每隔至少 5 分钟发送一个包;Sneaky,类似于 Paranoid,只是数据包的发送间隔是 15 秒;Polite,不增加太大的网络负载,避免宕掉目标

主机，串行每个探测，并且使每个探测有 0.4 秒的间隔；Normal，nmap 默认的选项，在不是网络过载或者主机/端口丢失的情况下尽可能快速地扫描；Aggressive，设置 5 分钟的超时限制，使对每台主机的扫描时间不超过 5 分钟，并且使对每次探测回应的等待时间不超过 1.5 秒；Insane，只适合快速的网络或者不在意丢失某些信息时，每台主机的超时限制是 75 秒，对每次探测只等待 0.3 秒。也可以使用数字来代替这些模式，例如，-T 0 等于-T Paranoid；-T 5 等于-T Insane。

这些适时模式不能和下面的适时选项组合使用。

(2) 参数：--host_timeout

设置扫描一台主机的时间，以毫秒为单位。默认的情况下，没有超时限制。

(3) 参数：--max_rtt_timeout

设置对每次探测的等待时间，以毫秒为单位。如果超过这个时间限制就重传或超时。默认值是大约 9000 毫秒。

(4) 参数：--min_rtt_timeout

当目标主机的响应很快时，nmap 就缩短每次探测的超时时间。这样会提高扫描的速度，但是可能丢失某些响应时间比较长的包。使用这个选项，可以让 nmap 对每次探测至少等待指定的时间，以毫秒为单位。

(5) 参数：--initial_rtt_timeout

设置初始探测的超时值。一般这个选项只在使用-P0 选项扫描有防火墙保护的主机才有用。默认值是 6000 毫秒。

(6) 参数：--max_parallelism

设置最大的并行扫描数量。--max_parallelism 1 表示同时只扫描一个端口。这个选项对其他的并行扫描也有效，例如，ping sweep 和 RPC scan。

(7) 参数：--scan_delay

设置在两次探测之间，nmap 必须等待的时间。这个选项主要用于降低网络的负载。

4) 目标设定

在 nmap 的所有参数中，只有目标参数是必须给出的。其最简单的形式是在命令行直接输入一个主机名或者一个 IP 地址。如果希望扫描某个 IP 地址的一个子网，可以在主机名或 IP 地址的后面加上掩码。掩码为/0 表示扫描整个网络，如果是/32 则表示仅扫描这个主机。使用/24 扫描 C 类地址，/16 扫描 B 类地址。除此之外，nmap 还有更加强大的表示方式来灵活地指定 IP 地址。采用 list/ranges 来为每个元素指定 IP 地址。例如，要扫描某个 B 类网络 128.210.*.*，可以使用下面三种方式来指定这些地址：128.210.*.*、128.210.0-255.0-255 或者 128.210.0.0/16，这三种形式是等价的。

通过详细讲述了 nmap 的参数后，下面结合具体例子来说明 nmap 的用法，设定目标主机为 target.example.com。现在，让 nmap 开始工作。

```
[root@ test root]#nmap -v target.example.com
```

扫描主机 target.example.com 的所有 TCP 端口。-v 打开冗余模式。

```
[root@ test root]#nmap -sS -O target.example.com/24
```

发起对 target. example. com 所在网络上的所有的 255 个 C 类 IP 地址的秘密 SYN 扫描。同时还探测每台主机操作系统的指纹特征,这个需要 root 权限来执行。

```
[root@ test root]#nmap -sX -p 22,53,110,143,4564 128.210.* .1-127
```

对 B 类 IP 地址 128.210 中 255 个可能的 8 位子网的前半部分发起圣诞树扫描。确定这些系统是否打开了 sshd、DNS、pop3d、imapd 和 4564 端口。注意圣诞树扫描对 Microsoft 的系统无效,因为其协议栈的 TCP 层有缺陷。

```
[root@ test root]#nmap -v --randomize_hosts -p 80 * .* .2.3-5
```

只扫描指定的 IP 范围,有时用于对这个 Internet 进行取样分析。nmap 将寻找 Internet 上所有后两个字节为.2.3、.2.4 或.2.5 的 IP 地址上的 Web 服务器。如果想发现更多有兴趣的主机,可以使用 127-222,因为在这个范围内有缺陷的主机密度更大。

```
[root@ test root]#host -l company.com | cut '-d' -f 4 | nmap -v -iL-
```

列出 company. com 网络上的所有主机,让 nmap 进行扫描。

**注意**:这个命令在 GNU/Linux 下使用。如果在其他平台,可能要使用其他的命令选项。现在 Windows 系统能够很好的支持 nmap 的运行,但 nmap 在 3.9 的版本后需要 WinPcap 的支持,用户可以先安装 WinPcap 后,安装运行 nmap。此外,有些防病毒软件(如 McAfee 防病毒软件)会把 nmap 视为一个潜在的威协。所以在必要的情况下,可以选用其他的防病毒软件以保证 nmap 能正常运行。

### 3. 端口扫描的防范

由于对目标主机进行端口扫描非常简单和方便,作为系统管理员或普通的用户都需要时刻关注所管理的机器的端口状况,要最大限度隐藏端口状况,减少不必要的安全漏洞。防范主机端口的非法扫描,可以从两个方面下手解决,一个是主机级的防范,一个是网络级的防范。对于主机级的防范,又可以从下面两个方面着手。

1) 关闭闲置和有潜在危险的端口

这个方法的本质就是将所有用户需要用到的正常计算机端口以外的其他端口都关闭掉,因为计算机的所有对外通信的端口都存在潜在危险,如果管理不善就会被入侵者利用,成为入侵的通道。在 Windows 系统中,可以将一些闲置的服务关闭掉,其对应的端口也就被同时关闭了。进入"控制面板"→"管理工具"→"服务"项内,关闭掉计算机的一些没有使用的服务(如 ftp 服务、dns 服务、iis admin 服务等),它们对应的端口也被停用了。如果用到"只开放允许端口的方式",可以利用系统网络设置中的"tcp/ip 筛选"功能实现,"只允许" 系统的一些基本网络通信需要的端口即可。

2) 对无法关闭的端口进行监控

有些端口是用户必需要用到的,而靠手工进行管理是不现实的,这就需要借助主机防火墙软件配合工作。主机防火墙会首先检查每个到达用户计算机的数据包,在这个数据包被计算机上运行的任何软件看到前,主机防火墙有完全的否决权,可以禁止用户计算机接收任何东西。当第一个请求建立连接的包被计算机回应后,一个 tcp/ip 端口被打

开。端口扫描时，对方计算机不断和本地计算机建立连接，并逐渐打开各个服务所对应的 tcp/ip 端口及闲置端口。防火墙经过自带的拦截规则判断，就能够知道对方是否正进行端口扫描，并拦截掉对方发送过来的所有扫描需要的数据包，现在市面上几乎所有网络防火墙软件都能够抵御端口扫描。

另外，由于源地址伪造是扫描技术的一个重要组成部分，源地址伪造是网上众多 DoS、DDoS 攻击的主要方法。一般情况下，可以通过以下两个方面来做好网络级的防御，一是通过路由器（或防火墙）过滤掉源地址是内部网络的外来包；二是通过路由器（或防火墙）过滤掉源地址不是内部网络的输出包。除此之外，一种较好的办法是采用入侵检测系统（IDS），入侵检测系统处于防火墙之后对网络活动进行实时检测。许多情况下，由于可以记录和禁止网络活动，所以可以认为入侵检测系统是防火墙的延续。它们可以和防火墙或路由器配合工作。入侵检测系统扫描当前网络的活动，监视和记录网络的流量，根据定义好的规则来过滤从主机网卡到网线上的流量，提供实时报警。网络扫描器只能检测主机上先前设置的漏洞，而 IDS 监视和记录网络流量，下面就一种常用的开源 IDS 系统进行说明。

#### 4. snort 的用法

入侵检测系统（IDS）是对计算机和网络系统资源上的恶意使用行为进行识别和响应的处理系统，在不影响网络性能的前提下，对网络进行警戒、检测。它具有监视分析用户和系统的行为、审计系统配置和漏洞、评估敏感系统和数据的完整性、识别攻击行为、对异常行为进行统计、自动的收集与系统相关的补丁、进行审计跟踪、识别违反安全法规的行为、使用骗诱服务器记录黑客行为等功能，使系统管理员可以比较有效地监视、审计、评估自己的系统。其基本功能与工作流程概括来说具有监控、分析用户和系统的活动，核查系统配置和漏洞，评估关键系统和数据文件的完整性，识别攻击的活动模式并向网管人员报警，对异常活动的统计分析，操作系统审计跟踪管理，识别违反政策的用户活动，并可用来评估重要系统和数据文件的完整性。

snort 是目前应用较为广泛的一个 IDS 产品，它被定位为一个轻量级的入侵检测系统。它以开放源代码形式发行，最初由 Martin Roesch 编写，并由遍布世界各地的众多程序员共同维护和升级。它支持多种系统软硬件平台，如 RedHat Linux、Solari、FreeBSD、NetBSD 以及 MacOS X 等。与许多昂贵且庞大的商用系统相比，snort 系统具有系统尺寸小、易于安装、便于配置、功能强大、使用灵活等优点。它采用基于规则的工作方式，对于数据包内容进行规则匹配来检测许多不同的入侵行为和探测活动。例如，缓冲区溢出、隐蔽端口扫描、CGI 攻击、SMB 探测等。snort 的工作流程可分成数据采集、数据分析和做出响应三部分。它首先采集来自网络系统不同节点（不同子网和不同主机）但隐藏了网络入侵行为的数据，如系统日志、网络数据包、文件与用户活动的状态和行为。接着通过模式匹配、异常检测或完整性分析等技术，对数据进行分析以寻找入侵。一旦发现入侵，IDS 就进入响应过程，并在日志、告警和安全控制等方面做出反应。

snort 可以实现对实时通信分析和信息包记录，对数据包有效载荷检查，进行协议分析和内容查询匹配，可以探测缓冲溢出、秘密端口扫描、CGI 攻击、SMB 探测、操作系统入

侵尝试。并可以对系统日志、指定文件、UNIX Socket 或通过 Samba 的 WinPopus 进行实时报警。snort 有三种主要工作模式：嗅探器(Sniffer)、记录器(Logger)或入侵探测系统(IDS)。

下面讲述 Linux 平台下 snort 的应用与配置，在 Linux 环境下需要事先安装多种软件构建支持环境才能使用 snort，如 zlib，LibPcap，MySQL，Apache 和 PHP4 等。安装过程比较复杂，这里着重讲述其如何应用，有关安装的内容可以参考相关内容。

1）snort 规则

snort 规则库是不断更新的，可以在 www. snort. org 上下载到最新的 snort 规则库。snort 使用一种简单的轻量级的规则描述语言来描述它的规则配置信息，灵活而强大。在版本 1.8 之前 snort 规则必须写在一个单行上，在现在的版本里可以用'\'来进行折行。

snort 规则分成两个逻辑部分：规则头和规则选项。规则头包含规则的动作、协议、源和目标 IP 地址与网络掩码以及源和目标端口信息。规则选项部分包含报警消息内容和要检查的包的具体部分。下面是一个规则范例。

```
alert tcp any any -> 192.168.1.0/24 111 (content: "|00 01 86 a5|"; msg: "mountd access";)
```

括号前的部分是规则头，括号内的部分是规则选项。规则选项部分中冒号前的单词称为选项关键字。

**注意**：不是所有规则都必须包含规则选项部分，选项部分只是为了使对要收集、报警或丢弃的包的定义更加严格。组成一个规则的所有元素对于指定的要采取的行动都必须是真的。当多个元素放在一起时，可以认为它们组成了一个逻辑与(AND)语句。同时，snort 规则库文件中的不同规则可以认为组成了一个大的逻辑或(OR)语句。以下面一条规则为例进行说明。

```
alert tcp $EXTERNAL_NET any - > $SQL_SERVERS 3306 (msg: "MYSQL root login attempt"; flow: to_server,
established; content: "|0A 00 00 01 85 04 00 00 80|root|00|"; classtype: protocol-comand-decode; sid:
1775;rev: 2;)
```

它表示从外部网络的任意端口访问 mysql 服务器的 3306 端口时，如果数据流里匹配到内容 0A 00 00 01 85 04 00 00 80 root 00(其中数字表示二进制字节码)，那么就在记录中或报警"MYSQL root login attempt"。通过对 snort 规则的分析，可以看出其实 snort 规则中除了 IP 地址和端口号以外，最重要的还是模式匹配的内容，即关键字 content 中包含的内容。要提交漏洞攻击代码和工具被利用时符合 snort 格式的网络检测特征，应该就是攻击代码中的特征字段。

通过对特征规则以及资料的分析，发现可以在运行攻击代码时用 sniffer 工具来截获数据包，然后根据数据包的解码内容来分析特征字段，提取匹配的要点，然后用 snort 中的关键字来书写规则，这样就得到了 snort 的特征规则。

2）snort 的工具和规则制定

snort 有三种工作模式：一是嗅探器模式(Sniffer Mode)，其作用是从网络中抓取数据包；二是分组日志模式(packet logger Mode)，其作用是将数据包记录到硬盘日志中；

三是网络入侵检测模式(network intrusion detection system Mode),其作用是分析网络中传输的数据并与入侵规则库相匹配来发现入侵行为。无论哪个工作模式都是用命令完成的,在具体介绍这些工作模式如何工作前,先介绍一下关于 snort 的命令。由于 snort 有比较多的命令选项和参数,要熟练使用 snort 就必须掌握这些选项。其通用形式为。

```
snort  -[options]
```

各个参数功能如下。

-A:选择设置警报的模式为 full、fast、unsock 和 none。full 模式是默认模式,它记录标准的 alert 模式到 alert 文件中;fast 模式只记录时间戳、消息、IP 地址和端口信息到文件中;unsock 模式是发送到 UNIX socket;none 模式是关闭报警。

-a:显示 ARP 包。

-b:以 tcpdump 格式记录 LOG 的信息包,所有信息包都被记录为二进制形式。用这个选项记录速度相对较快,因为它不需要将信息转化为文本。

-c:使用配置文件。这个规则文件是告诉系统信息是要记录日志,还是报警或是通过。

-C:只用 ASCII 码来显示数据报文负载,不用十六进制。

-d:显示应用层数据。

-D:以守护进程的形式运行。默认情况下警报将被发送到/var/log/snort.alert 文件中去。

-e:显示并记录第二层信息包头的数据。

-F:从文件中读 BPF 过滤器(filters)。

-g:程序初始化后使用用户组标志(group ID)。这种转换使得 snort 不必在初始化时必须使用 root 用户权限,从而提高了系统的安全性。

-h:使用这个选项 snort 会用箭头的方式表示数据进出的方向。

-i:在网络接口上监听。

-I:添加第一个网络接口名字到警报输出。

-l:把日志信息记录到目录中去。

-L:设置二进制输出的文件名。

-m:设置所有 snort 输出文件的访问掩码。

-M:发送 WinPopup 信息到包含文件中的工作站列表中去,此选项需要 Samba 的支持。

-n:是指定在处理若干个数据包后退出。

-N:关闭日志记录,但 ALERT 功能仍旧正常工作。

-o:改变规则应用到数据包上的顺序,正常情况下采用 Alert→Pass→Log order,而采用此选项后的顺序是 Pass→Alert→Log order。其中 Pass 是那些允许通过的规则,ALERT 是不允许通过的规则,LOG 指日志记录。

-O:使用 ASCII 码输出模式时,本地网 IP 地址被代替成非本地网 IP 地址。

-p：关闭混杂(Promiscuous)嗅探方式。

-P：设置 snort 的抓包截断长度。

-r：读取 tcpdump 格式的文件。

-s：把日志警报记录到 syslog 文件。在 Linux 中警告信息会记录在/var/log/secure，在其他平台上将记录在/var/log/message 中。

-S：设置变量 n=v 的值，用来在命令行中定义 snort rules 文件中的变量，如要在 snort rules 文件中定义变量 HOME_NET，可以在命令行中给它预定义值。

-t：初始化后改变 snort 的根目录到目录。

-T：进入自检模式，snort 将检查所有的命令行和规则文件是否正确。

-u：初始化后改变 snort 的用户 ID 到指定值。

-v：显示 TCP/IP 数据包头信息。

-V：显示 snort 版本并退出。

-y：在记录数据包信息的时间戳上加上年份。

-?：显示 snort 简要的使用说明并退出。

除了少数几个不常用的命令，大部分的命令都在这里。掌握这些命令后，可以根据自己的需要来选择使用不同的工作模式。下面来看看这三种工作模式是如何具体工作的。

3) snort 的工作模式

(1) 嗅探器模式

snort 使用 Libpcap 包捕获库，即 TCPDUMP 使用的库。在这种模式下，snort 使用网络接口的混杂模式读取并解析共享信道中的网络分组。

```
[root@ localhost root]#snort -v
```

显示 TCP/IP 等的网络数据包头信息在屏幕上。

举例如下。

```
[root@ localhost root]#snort -vd
```

显示较详细的包括应用层数据传输的信息。

```
[root@ localhost root]#snort -vde
```

显示更详细的包括数据链路层的数据信息。

(2) 日志模式

上面介绍的嗅探器模式的几个命令都只把信息显示在屏幕上，而如果要把这些数据信息记录到硬盘上的指定目录中，那就需要使用 Packet Logger 模式。

```
[root@ localhost root]#snort -vde -l ./log
```

把 snort 抓到的数据链路层、TCP/IP 报头、应用层的所有信息存入当前文件夹的 log 目录中。这里的 log 目录可以根据自己的需要而更换。

```
[root@ localhost root]#snort -vde -l ./log -h 192.168.1.0/24
```

记录192.168.1.0/24这个C类网络的所有进站数据包信息到log目录中去，log目录中的子目录按计算机的IP地址来命名。

```
[root@ localhost root]#snort -l ./log -b
```

记录snort抓到的数据包并以TCPDUMP二进制的格式存放到log目录中去，而snort一般默认的日志形式是ASCII文本格式。ASCII文本格式便于阅读，二进制的格式转化为ASCII文本格式无疑会加重工作量。所以在高速的网络中，由于数据流量太大，应该采用二进制的格式。

```
[root@ localhost root]#snort -dvr packet.log
```

此命令不是存储日志，而是读取“packet.log”日志中的信息到屏幕上。

(3) 网络入侵检测模式(NIDS)

网络入侵检测模式是用户最常用到的模式，是用户需要掌握的重点。这种模式其实混合了嗅探器模式和分组日志模式，并且需要载入规则库才能工作。

```
[root@ localhost root]#snort -vde -l ./log -h 192.168.1.0/24 -c snort.conf
```

载入snort.conf配置文件，并将192.168.1.0/24网段的报警信息记录到./log中去。这里的snort.conf文件可以换成自己的配置文件。载入snort.conf配置文件后，snort将会应用在snort.conf中的规则去判断每一个数据包以及性质。如果没有用参数－l指定日志存放目录，系统默认将报警信息放入/var/log/snort目录下。如果没有记录链路层数据的需要或要保持snort的快速运行，可以把-v和-e关掉。

关于网络入侵检测模式，还有一个地方要注意的是它的警报输出选项，在前面已经介绍了snort有多种警报的输出选项，这里再具体讲讲如何使用。

```
[root@ localhost root]#snort -A fast -l ./log -h 192.168.1.0/24 -c snort.conf
```

载入snort.conf配置文件，启用fast警报模式，以默认ASCII格式将192.168.1.0/24网段的报警信息记录到. /log中去。这里的fast可以换成full或none等，但在大规模高速网络中最好用fast模式。

```
[root@ localhost root]#snort -s -b -l ./log -h 192.168.1.0/24 -c snort.conf
```

以二进制格式将警报发送给syslog，其余的与上面的命令一样。要注意的是警报的输出模式虽然有六种，但用参数-A设置的只有4种，输出到syslog用参数-s，smb模式使用参数-M。

### 3.3.2 网络监听原理及其工具

网络监听工具又被称为嗅探器(Sniffer)，它是一种利用计算机网络接口截获目的计算机数据报文的技术，其目的就是截获通信的内容，其手段是对协议进行分析。由于网络监听操作简单，很多入侵者利用它来进行网络入侵渗透。网络监听对于安全的威胁来自于其被动性和非干扰性，它往往让网络信息泄密变得不容易发现。监听器工作在网络的底层，在某个广播域中进行数据包监听，它将网络传输的数据记录下来，管理员可以利

用这些记录分析流量，查找网络漏洞，检测网络性能，以便找出网络中可能存在的安全问题。而入侵者同样也能通过对这些捕获的数据进行分析，从而获得网络上传输的一些重要信息，特别是用户的密码。事实上，很多黑客入侵时都把局域网扫描和监听作为实施入侵的最基本步骤和手段，试图用这种方法获取用户的密码等信息。此外，如果要对入侵活动和其他网络犯罪进行侦查、取证时，也可以使用网络监听技术来获取必要的信息，所以了解网络监听的技术原理、实现方法和防范措施，对于网络安全管理是非常重要的。

Sniffer 软件本身处于数据链路层之上，同物理层和数据链路层无关。因此，Sniffer 软件可以运行在各种数据链路层的协议和物理传输介质上，如图 3-11 所示。不同传输介质的网络可监听性是不同的，由于以太网是一个广播型的网络，所以其被监听的可能性比较高。FDDI Token 尽管并不是一个广播型网络，但带有令牌的那些数据包在传输过程中，平均要经过网络上一半的计算机，所以其被监听的可能性也比较高。微波和无线网被监听的可能性同样比较高，因为无线电本身是一个广播型的传输介质，弥散在空中的无线电信号可以被很轻易的截获。一般情况下，大多数的 Sniffer 系统能够分析 TCP/IP、IPX、DECNET、FDDI Token 及微波和无线网。

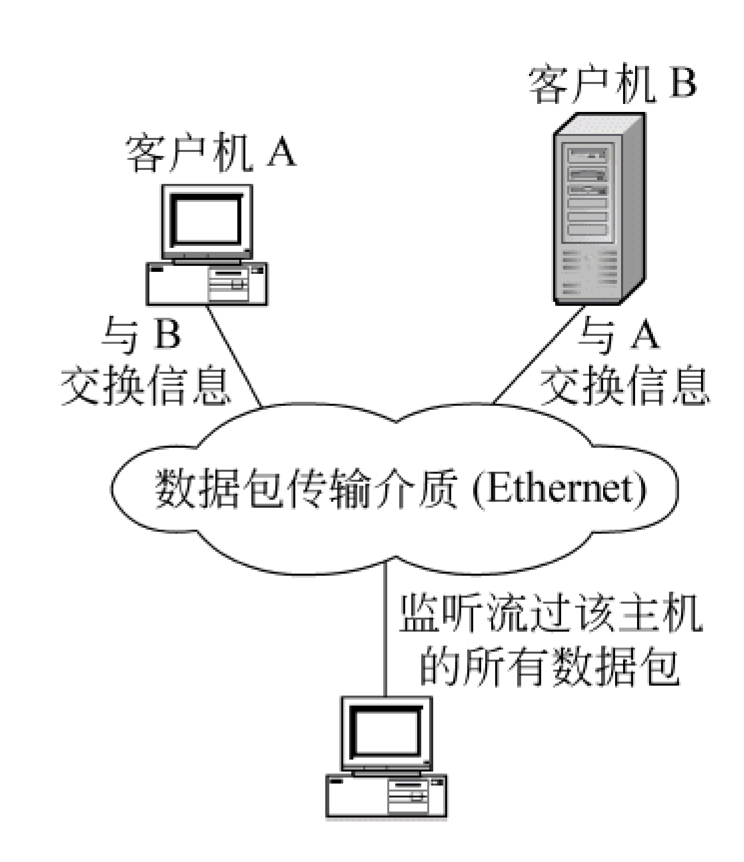



**图 3-11 Sniffer 在以太网下的工作原理**

由于以太网目前应用最为广泛，故重点分析以太网的监听原理与应用。在以太网中，所有的通信都是广播的，也就是说通常在同一个网段的所有网络接口都可以访问在物理媒体上传输的所有数据。每一个网络接口都有一个唯一的硬件地址，这个硬件地址也就是网卡的 MAC 地址，大多数系统使用 48 比特的地址，这个地址用来表示网络中的每一个设备。一般来说每一块网卡上的 MAC 地址都是不同的，在硬件地址和 IP 地址间使用 ARP 和 RARP 协议进行相互转换。在正常的情况下，一个网络接口只响应与自己硬件地址相匹配的数据帧和发向所有机器的广播数据帧。当网卡接收到传输来的数据，网卡内的单片程序会接收数据帧的目的 MAC 地址，根据网卡驱动程序设置的接收模式判断该不该接收，如认为该接收就接收，然后产生中断信号通知 CPU，如认为不该接收就丢掉不管，因此，不该接收的数据网卡就截断了，计算机根本就不知道。CPU 得到中断信号产生中断，操作系统就根据网卡驱动程序设置的网卡中断程序地址调用驱动程序接收数据，驱动程序接收数据后放入信号堆栈让操作系统处理。而对于网卡来说一般有四种接收模式。

(1) 广播方式：该模式下的网卡能够接收网络中的广播信息。

(2) 组播方式：设置在该模式下的网卡能够接收组播数据。

(3) 直接方式：在这种模式下，只有目的网卡才能接收该数据。

(4) 混杂模式：在这种模式下，网卡能够接收一切通过它的数据，而不管该数据是否是传给它的。

Sniffer 将以太网卡设置成混杂模式来捕获网络上所有的报文和数据帧。通过网络监听这些数据，可以从中捕获用户密码，捕获专用的或者机密的信息，可以用来危害网络

应用的安全，当然也可以用来获取更高级别的访问权限以及分析网络结构，进行网络渗透。在实际的应用中，Sniffer 分为硬件和软件两种。Sniffer 硬件通常称为协议分析仪，从协议分析仪发展的角度来说，如何对这些捕获到的数据进行分析、分类统计和发现并报告错误是网络管理过程中更需要关注的问题。网络维护人员越来越需要使用功能强大并能将多种网络测试手段集于一身的综合式测试分析手段，典型的协议分析仪上的功能延展就是加入网管功能、自动网络信息搜集功能、智能的专家故障诊断功能，并且移动性能要有效。这种综合的协议分析仪或者说是综合的网络分析仪成为了当今网络维护和测试仪的主要发展趋势，像 Fluke 的协议分析仪在网络现场分析、故障诊断和网络维护方法得到了相当广泛的应用和发展。随着网络维护规模的加大，以及网络技术的变化，网络关键数据的采集也越来越困难。有时为了分析和采集数据，必须能在异地同时地进行采集，于是要将协议分析仪的数据采集系统独立开来，能安置在网络的不同地方，由能控制多个采集器的协议分析仪平台进行管理和数据处理，这种应用模式就诞生了分布式协议分析仪。通常这种方式的分析仪造价非常高，从一定程度上限制了普通网络管理人员的使用，图 3-12 为 OptiView Series Ⅲ分析仪。

尽管 Sniffer 软件往往无法捕获网络上所有的传输数据（比如碎片数据），无法全面了解网络的故障和运行情况。但其易于使用，价格便宜，而且还有许多是开放源代码的开源软件，因此 Sniffer 软件在网络管理中得到了更为广泛的应用，如 Windows 系统下的 Sniffer Pro 和 NetXRay，Solaris 下的 Nfswatch 以及 UNIX/Linux 下的 Tcpdump 和 Sniffit 等。Sniffer 软件应用广泛，种类也较多，下面介绍几种常用的 Sniffer 软件工具的使用方法。



**图 3-12　OptiView Series Ⅲ分析仪**

### 1. Sniffer Pro

Sniffer Pro 是美国 Network Associates 公司出品的一款强大的网络分析工具软件，在网络管理中得到了应用广泛，是传统的网络管理工具。利用这个工具，能够捕获网络数据包来进行详细分析，使用专家系统对网络故障进行诊断，可实时监控网络运行状况，可以对网络中单独的工作站、会话或其他部分挑选详细的使用与差错统计，可以保存历史记录来进行基础分析，还可以产生可视与可听的实时报警来通知管理员，可以使用内置的工具软件模拟网络流量，测量响应时间等来刺探网络。Sniffer Pro 可以让用户运行多个程序及其工具的实例，还可以与其他 Windows 应用程序同时运行。由于它采用了直观的 Windows 用户界面，它的学习和使用比较简单，下面将详细介绍其使用及配置方法。

1）系统的安装与运行

Sniffer Pro 软件安装在 Windows 操作系统上，安装过程简单。在系统安装提示完成后，运行程序后出现图 3-13 所示的主界面。需要在进行流量捕获之前先选择网络适配器，确定从计算机的哪个网络适配器上接收数据。一般第一次启动软件时，会自动要求

选择相应的网络适配器，还可以通过 File→select settings 来进行选择，如图 3-14 所示。只有选择了网络适配器后才能正常工作，如果需要也可以选择拨号适配器对窄带拨号进行操作。如果安装了 EnterNet500 等 PPPOE 软件还可以选择虚拟出的 PPPOE 网卡。安装在 Windows 2000/XP 上的无上述功能，这和具体的操作系统有关。

Sniffer Pro 栏目上的目录菜单包括“文件”、“监控”、“捕获”、“显示”、“工具”、“数据库”、“窗口”和“帮助”8 大部分。在相应的目录菜单下，可以根据需要对一些选项进行配置。单击“开始”按钮，程序会开始对包进行捕获。

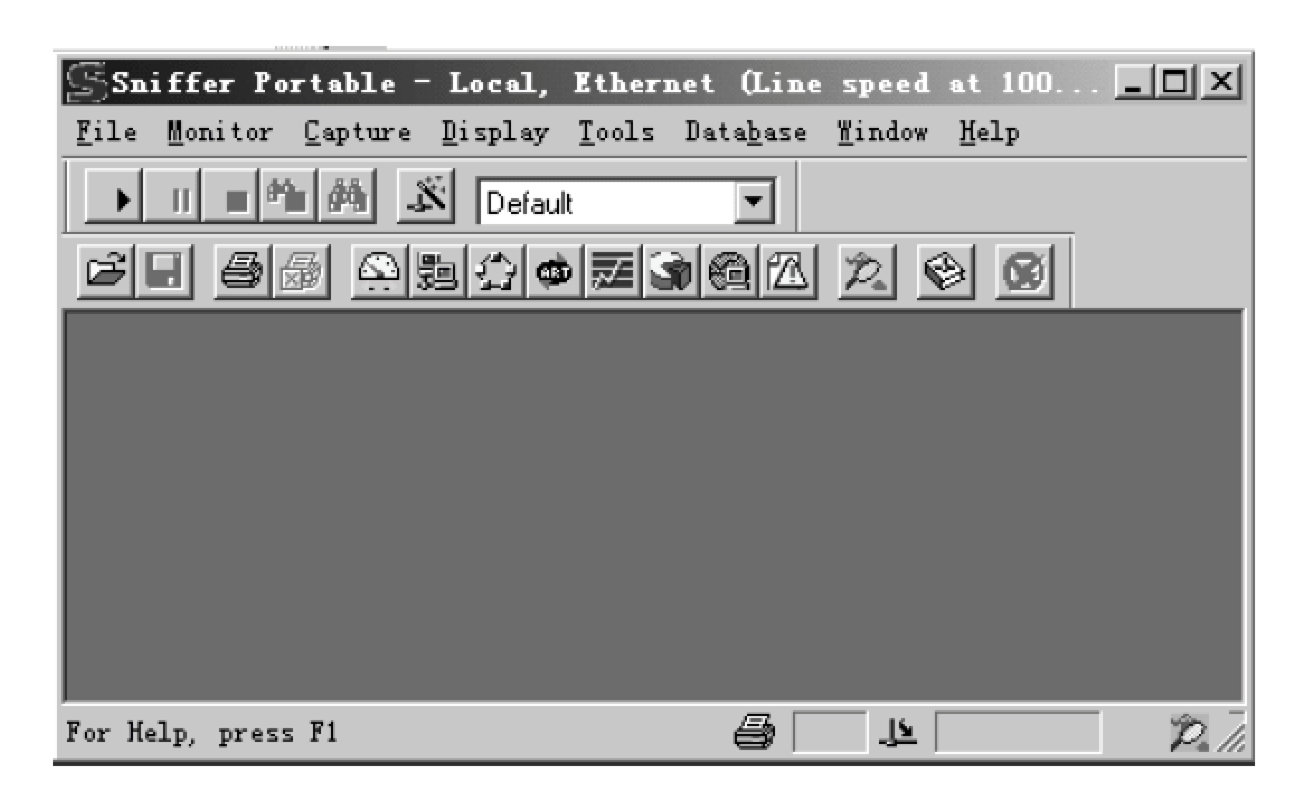



**图 3-13 Sniffer Pro 控制面板**

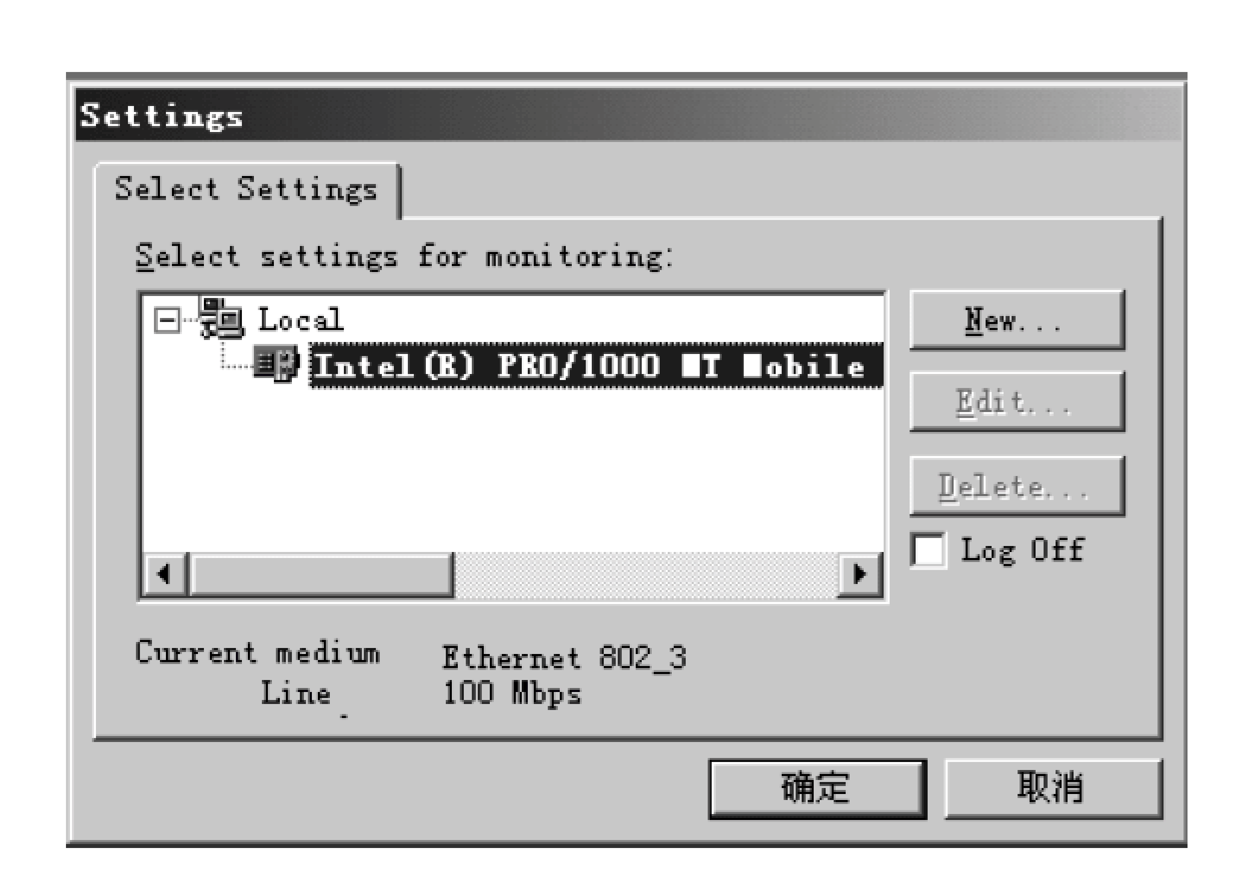



**图 3-14 选择网络适配器**

2) 监控网络运行

网络监视功能能够时刻监视网络，统计网络上资源的利用率，并能够监视网络流量的异常状况。这里只介绍一下 Dashboard 和 ART，其他功能比较简单可以参看在线帮助或直接使用即可。可以通过快捷键进入 Dashboard(仪表盘)选项，如图 3-15 所示。利用 Dashboard 可对网络运行状况进行实时查看，如系统利用率、转发率和出错率。还可以提供详细的网络统计报表，当然也可以方便地选择需要显示的数据，如丢包率、比特率等。Sniffer Pro 还提供了丰富的显示与统计功能，例如，可以通过选择“监控”→“全局状态”来查看数据包的大小分布，提供了条状图和饼图来进行显示。系统还提供了主机表，用以实时显示主机进出数据包的大小、差错率等，可以查看 IP、IPX、SDLC、ATMCNX 等。

可以通过选择需要显示的节点数，默认情况下系统显示 10 个流量最大的节点。

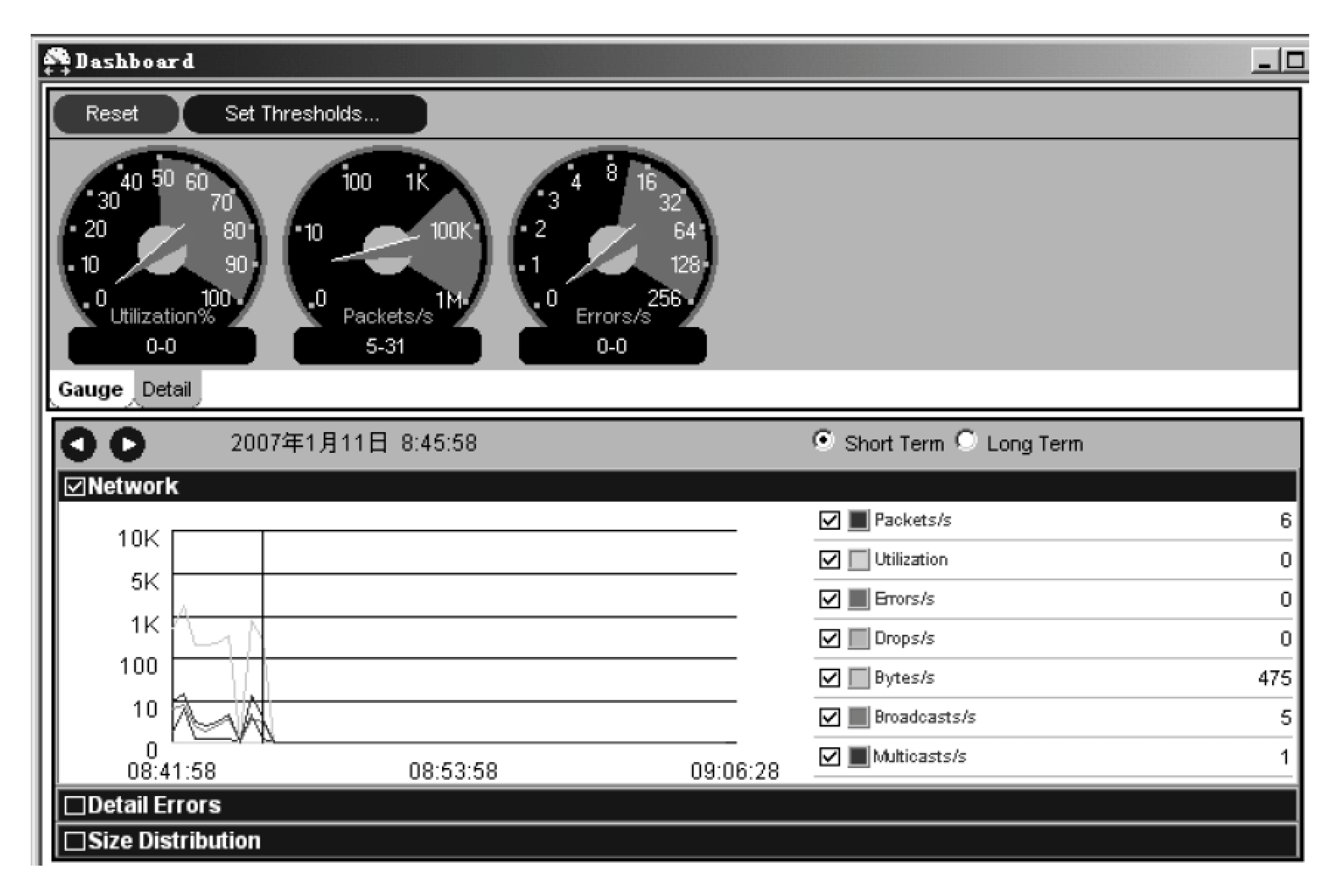



图 3-15 Dashboard 显示

Sniffer Pro 还能通过 Matrix(矩阵)显示网络流量，可以通过地图或表格来测量网络流量，显示目的地址和源地址的 IP 或 MAC，如图 3-16 和图 3-17 所示。还能统计出流量最高的 10 个会话，通过流量分析可以对网络状况进行一个简单的了解。

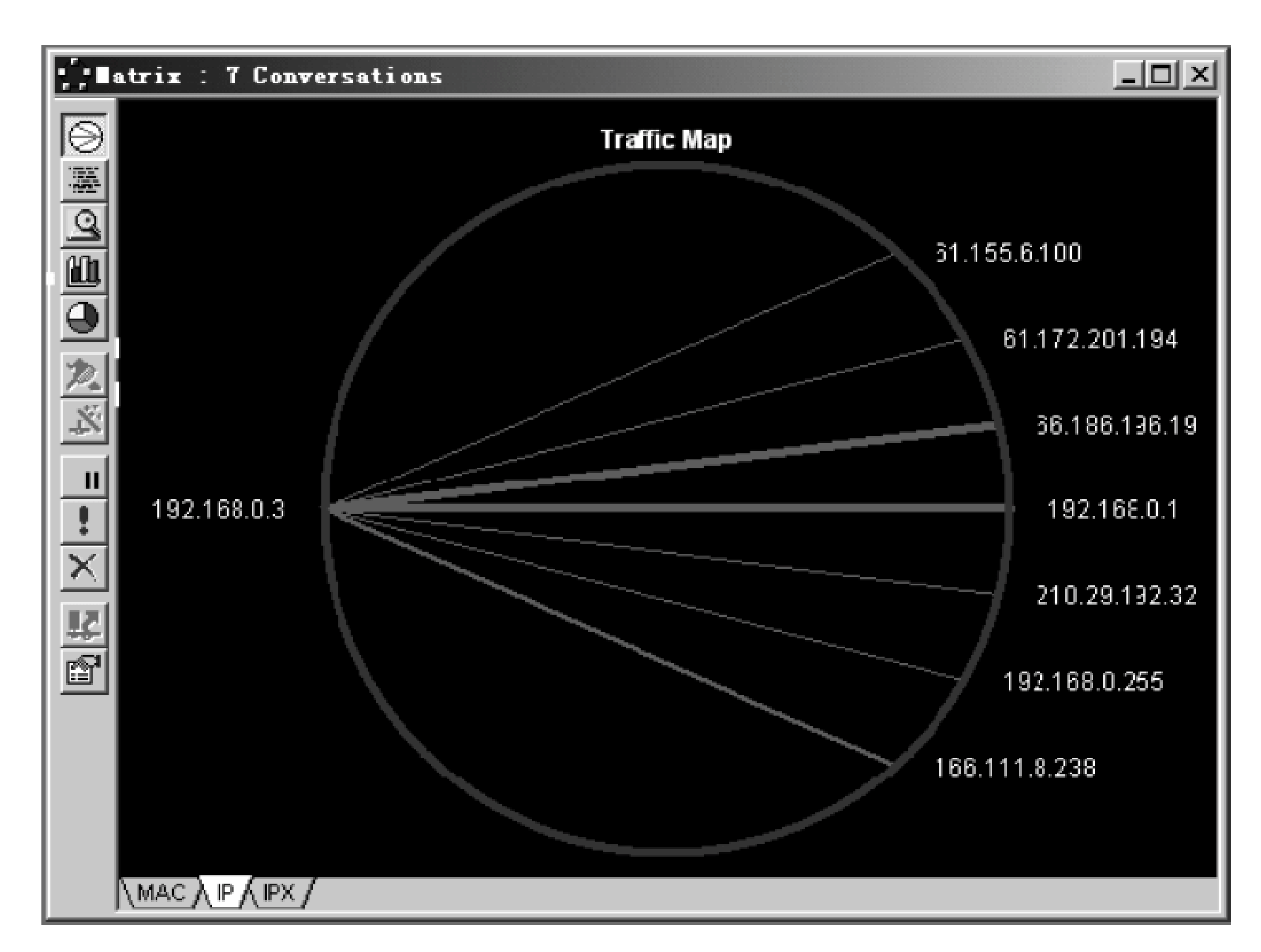
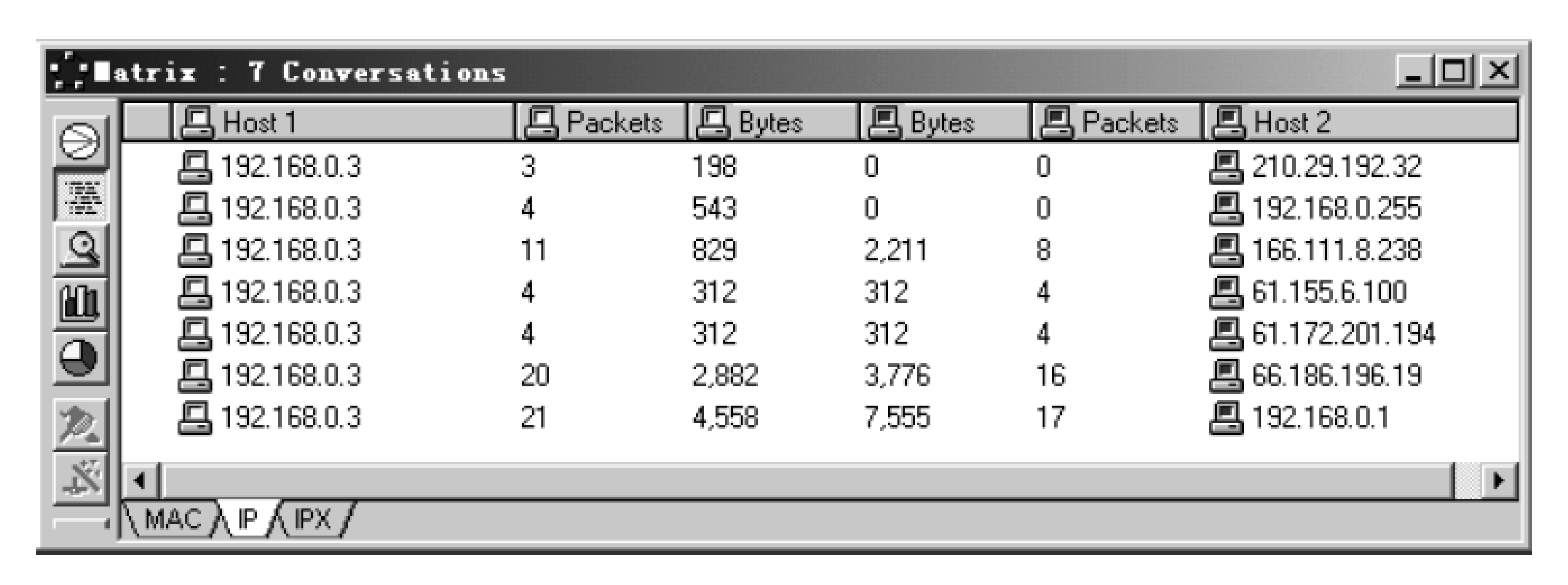



图 3-16 地图方式显示

除了显示网络流量外，系统还提供基于网络层的协议(如 IPX/SPX、TCP/IP、NetBIOS 等)的实时显示，并支持 TCP/IP 应用分布图，还能监控一些流行的应用，如 FTP、HTTP、Telnet、SMTP、POP 等。当然，对于 IPX 和 ATM 也能提供相应的统计查看功能。通过查看协议分布快捷按钮，就能以条状图、饼图或表的格式对各种协议应用



Matrix : 7 Conversations

| Host 1 | Packets | Bytes | Bytes | Packets | Host 2 |
|---|---|---|---|---|---|
| 192.168.0.3 | 3 | 198 | 0 | 0 | 210.29.192.32 |
| 192.168.0.3 | 4 | 543 | 0 | 0 | 192.168.0.255 |
| 192.168.0.3 | 11 | 829 | 2,211 | 8 | 166.111.8.238 |
| 192.168.0.3 | 4 | 312 | 312 | 4 | 61.155.6.100 |
| 192.168.0.3 | 4 | 312 | 312 | 4 | 61.172.201.194 |
| 192.168.0.3 | 20 | 2,882 | 3,776 | 16 | 66.186.196.19 |
| 192.168.0.3 | 21 | 4,558 | 7,555 | 17 | 192.168.0.1 |

MAC IP IPX

图 3-17 表格方式显示

进行直观显示。图 3-18 就是一个协议分布的条状图。为了过滤掉一些冗余的流量信息，可以利用过滤器来将一些协议或应用进行过滤。

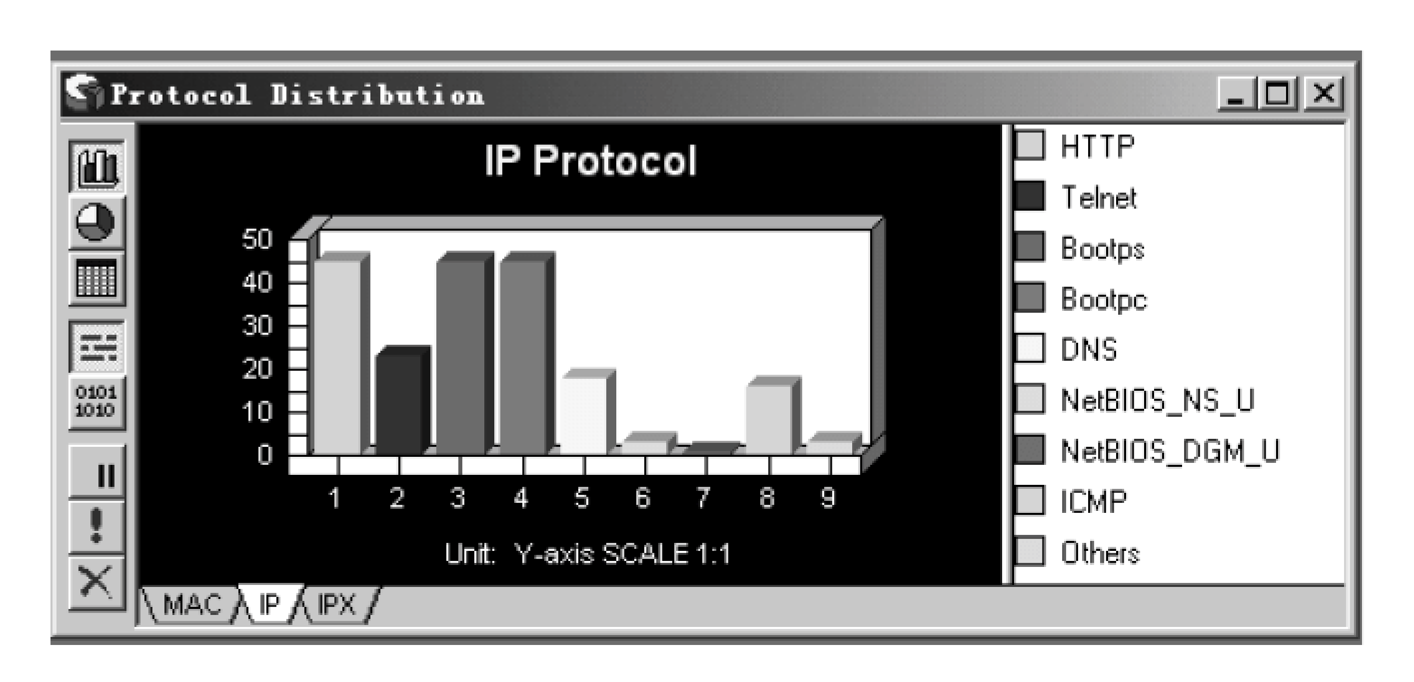



图 3-18 协议分布图

对于一些常见的 TCP/UDP 端口上的服务器与客户机之间的应用层链接(如 HTTP、FTP、DNS 等)，应用程序响应时间(application response time，ART)可实时测量并报告其响应时间。响应时间是指从请求发出到 Sniffer Pro 发现相应的响应之间的时间。可以在参数控制里选择需要监控的协议，如图 3-19 所示。

ART Options

General | Server-Client | Servers Only | Display Protocols

| | Name | Show ART |
|---|---|---|
| 1 | HTTP | ☒ |
| 2 | FTP_Data | ☐ |
| 3 | FTP_Ctrl | ☐ |
| 4 | NNTP | ☐ |
| 5 | POP | ☐ |
| 6 | POP3 | ☒ |

TCP UDP

确定 取消

图 3-19 ART Options 参数选项

如果希望了解 HTTP、POP3、SMTP、Telnet 的应用状况，可以选取这四项协议进行查看。打开 ART 运行一段时间后，可以看到如图 3-20 所示的统计表。这个统计表清楚地表明了这些应用的响应时间，对于了解网络应用很有帮助。ART 应用程序除了能测

量和报告应用程序响应时间外，还能在检测到应用程序响应时间大于所设定的阈值时自动生成警报。生成的警报会写入警报日志，并根据设置采取相应的警报处理方式。

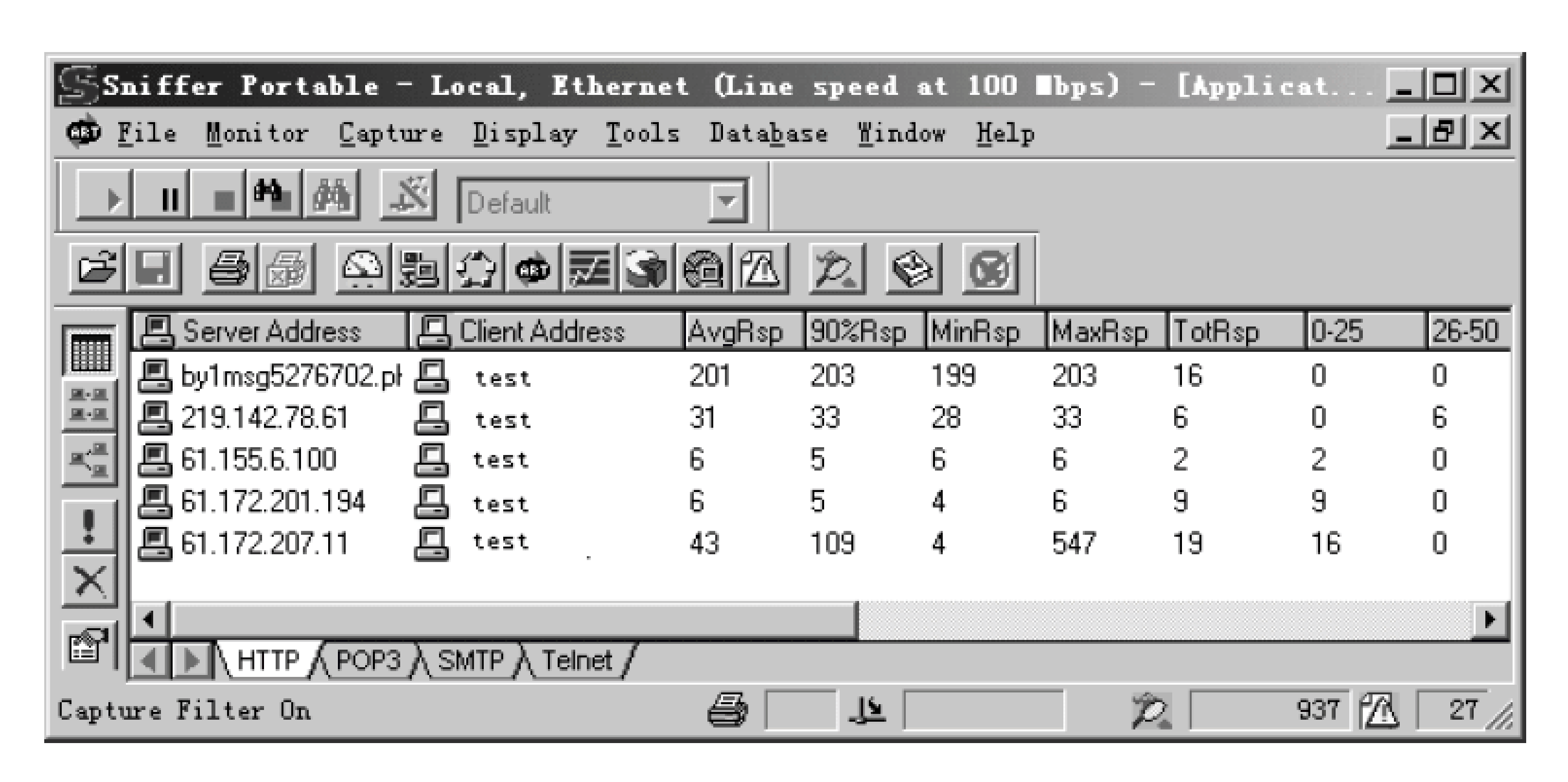


图 3-20　ART 显示

3）报文捕获

Sniffer Pro 具有强大的报文捕获能力。捕获功能与存储网络通信量测量及计算数据的监控功能不同，它是从网络中采集数据包并将其存储在捕获缓冲中。在捕获过程中，专家系统将分析数据包并实时显示分析结果。在停止捕获后，可通过 Sniffer Pro 的显示功能对捕获的数据包进行解码加以显示，还可提供专家系统的分析结果。在捕获过程中可以通过仪表盘面板查看捕获报文的数量和缓冲区的利用率，如图 3-21 所示。可以根据不同的要求对协议、流量图、应用程序等进行实时的监听。捕获到的数据包存储在捕获缓冲区中，可以显示和分析其中的数据包或者将数据包存到磁盘，也可以加载和显示以前保存的捕获文件，甚至还可以将捕获的数据包实时假脱机到文件，以有效增加捕获缓冲区的容量。

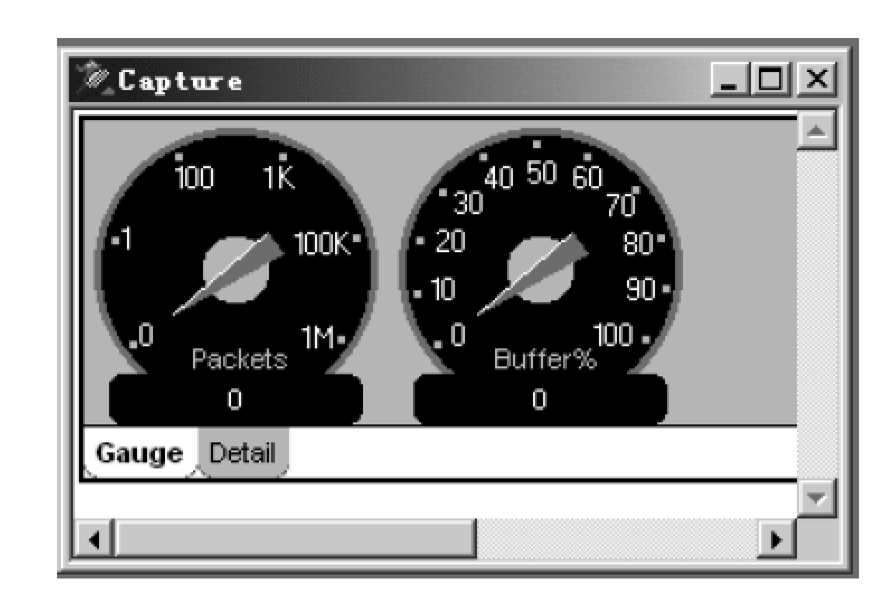


图 3-21　捕获面板

4）专家系统

为了有效进行网络分析，需要根据网络的协议环境在开始捕获数据前配置专家系统。在捕获过程中，专家系统将通过其监控的通信量构建数据库，并根据网络故障所在的专家系统层对其进行归类。可以根据具体要求，利用专家系统的配置选取特定的通信进行分析，并指定数据库中可为每个专家系统层创建的最大对象数和在专家系统中可创建的最大警报数。当达到最大警报数后，专家系统将重用最早、优先级最低的警报。要配置对象和专家系统选项，请选择工具菜单中的专家系统选项，如图 3-22 所示。

用户还可以对报警、子网掩码、802.11、协议等进行设置。需要注意的是，如果网络中使用不规范的子网掩码时，必须为网络添加 IP 地址和相应的子网掩码，以使专家系统能找到数据帧。专家系统将在捕获过程中执行 RIP（路由信息协议）分析，通过分析所捕获帧中的 RIP 以及其他路由协议来构建路由表，用于检测常见的路由选择故障。专家系统将跟踪网络上发现的路由器及配置的默认路由器。对于专家系统要分析的 RIP 数据

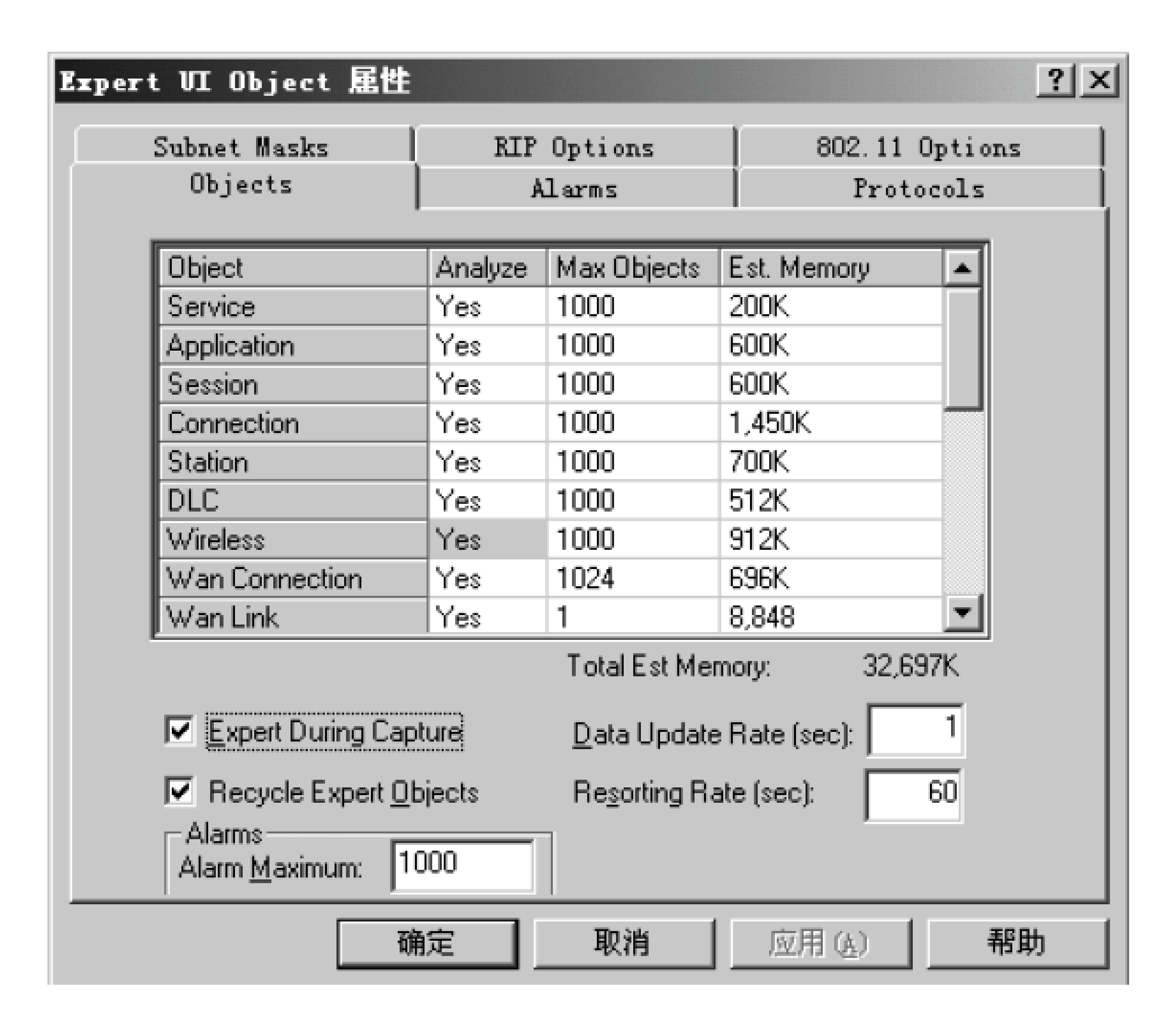



图 3-22　专家系统参数选项

包,必须在“专家系统属性”对话框的“对象”选项卡上将连接层或应用层设置为“分析”,因为 RIP 位于 UDP 之上,因此要从 UDP 解释器调用 RIP 解释器,而 Sniffer Pro 将 UDP 视为传输层,所以要分析传输层及以上层,至少应选中连接层,如图 3-23 所示。

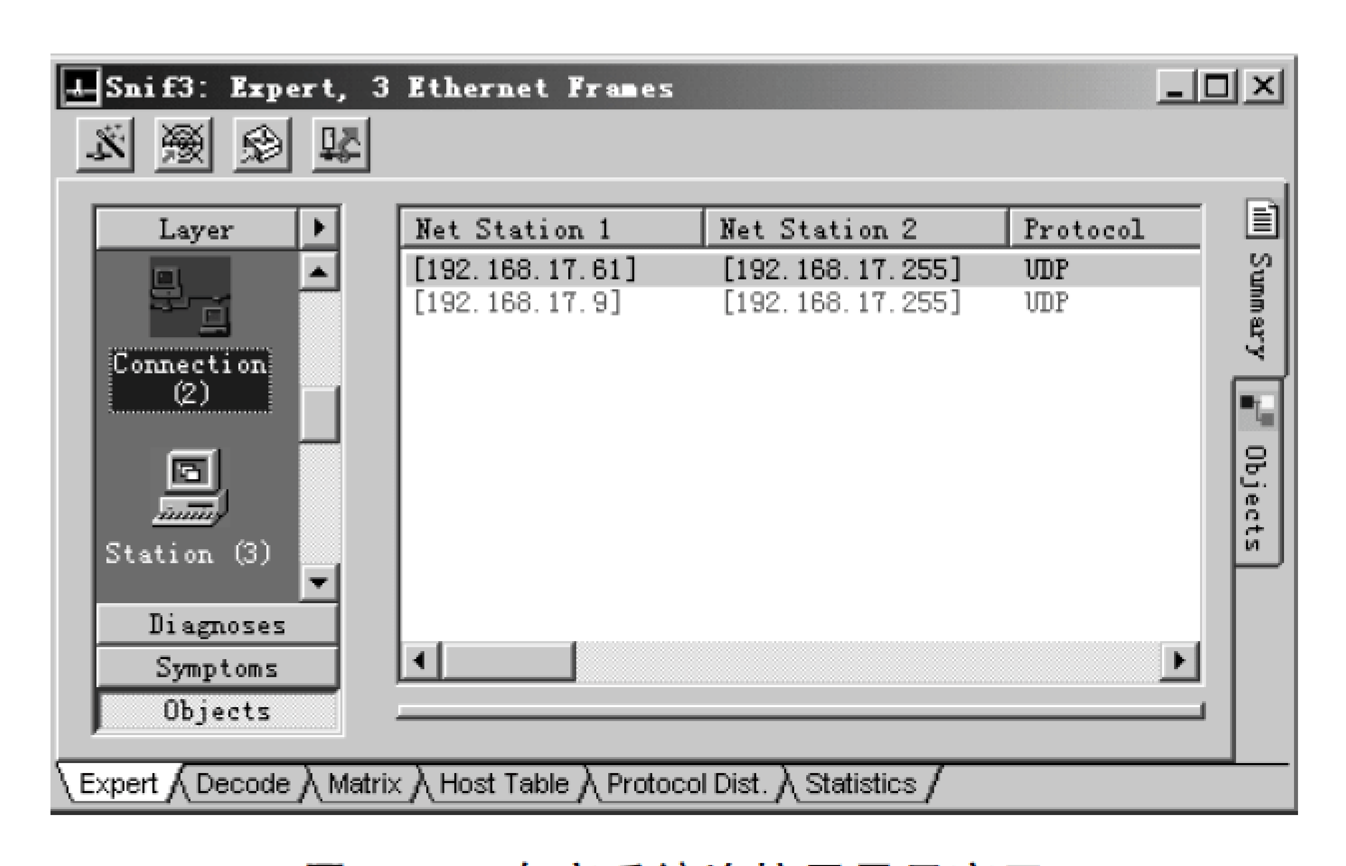



图 3-23　专家系统连接层显示窗口

专家系统分析期间,Sniffer Pro 将根据发现的通信量构建网络对象的数据库。专家系统协议解释器可以获得缓冲区中主机连接的所有信息。用户可以通过专家系统的显示筛选,自动显示捕获缓冲区中与特定项相关的所有通信量。专家系统分析器可采用多种算法来判断哪些帧可能会与网络对象关联,还扼要地解释了每个生成的症状和诊断,如图 3-24 所示。在捕获过程中,专家系统将根据所发现的帧创建专家系统对象。对于长时间的捕获,专家系统对象所用的某些帧很可能已从捕获缓冲区中消失,因为要给新的数据腾出空间。

5) 报文分析与解码

要显示捕获缓冲区及相关专家系统分析的内容,可以在捕获过程中单击主工具栏的

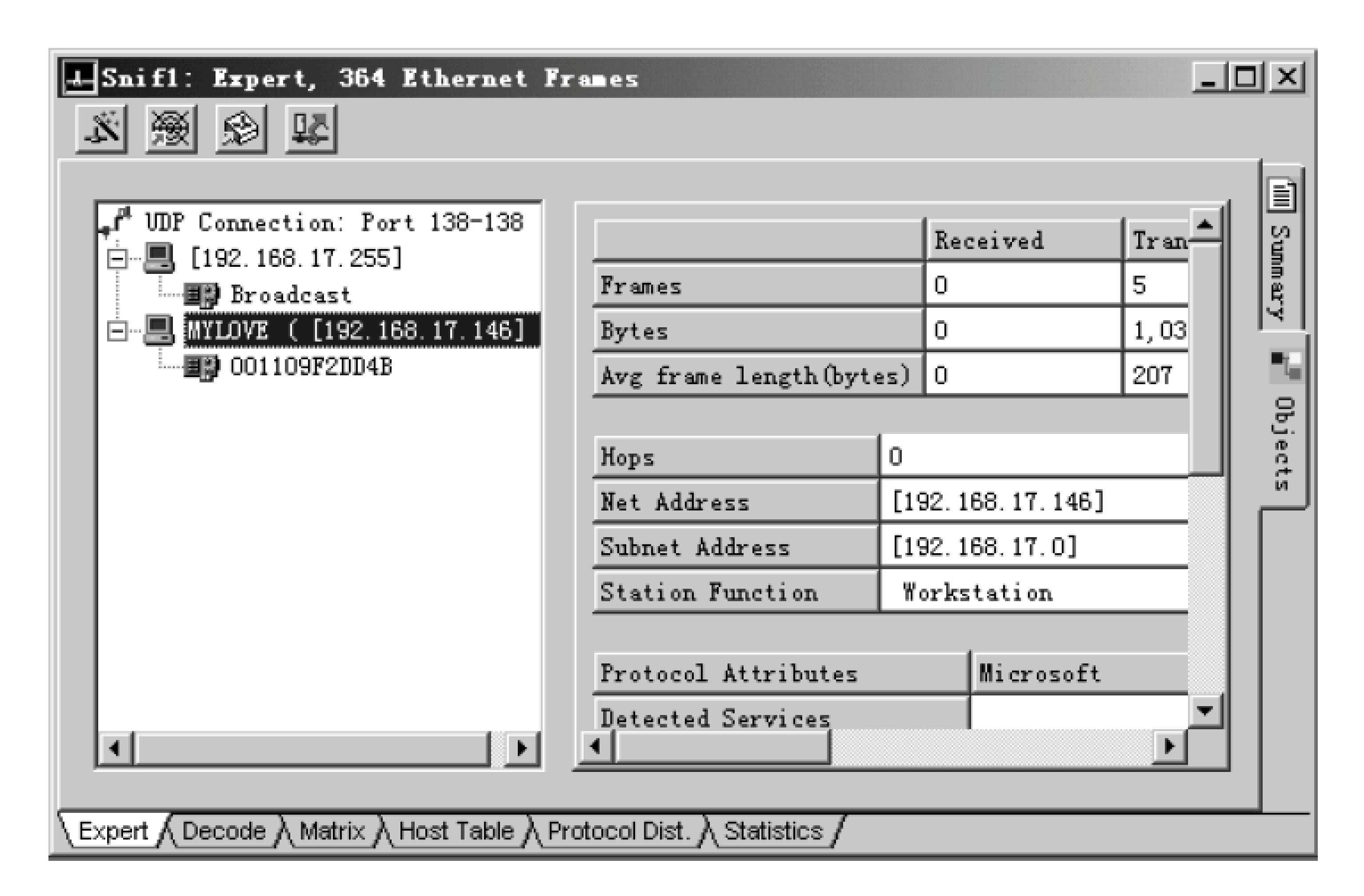



图 3-24 详细显示专家系统连接状况

“停止并显示”按钮。当开始实时显示专家系统分析的捕获时，专家系统显示也会打开。当首次查看捕获结果时，“专家系统显示”将显示所有在捕获会话过程中分析的通信量。在显示解码数据包和专家系统分析前，可以应用显示筛选，并配置专家系统选项，确定专家系统数据显示方式，使用户可查看网络分析所需的特定数据。在显示捕获缓冲区的内容时，Sniffer Pro 将使用它的协议解释器解释并解码捕获数据包中的高层协议，其可以解码 200 多种网络协议。“解码”选项卡在三个查看窗格中使用不同颜色表示数据包，如图 3-25 所示。摘要窗口用来逐行显示所捕获的数据包摘要信息。详细信息窗口显示了“摘要”窗口中当前所选数据包的详细内容，每一层协议都进行了解释和显示。十六进制窗口以十六进制和 ASCII 格式显示所选取的数据包，可以发现协议字段与它在数据包中

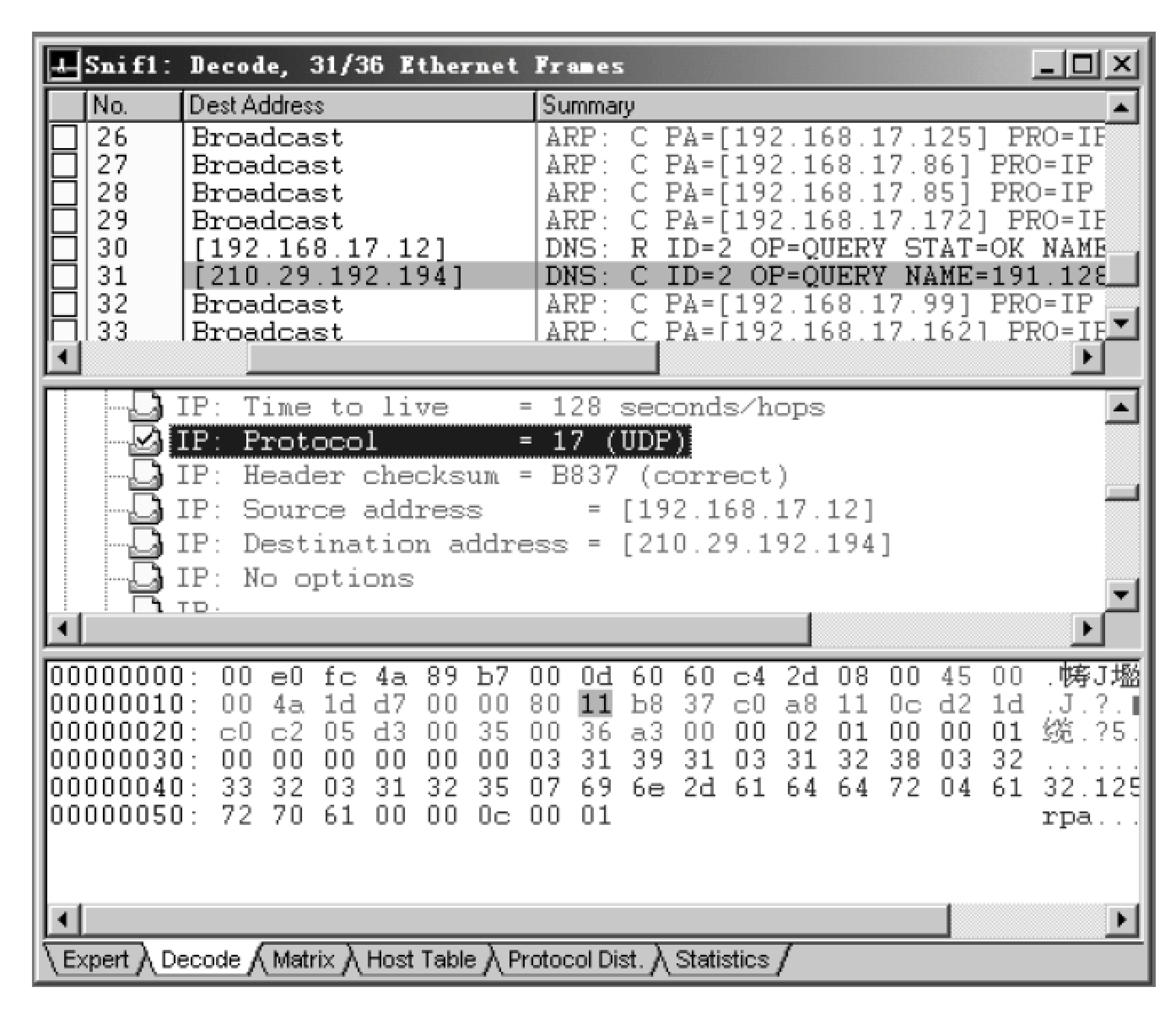



图 3-25 解码显示及示意图

相应字节的对应关系。

由于解码器显示可能包括大量的数据帧，就需要通过 Sniffer Pro 强大的搜索功能来进行筛选。可以在解码显示中搜索与文本字符串、某种数据模式、某种状态标志匹配的帧或者搜索与某个专家系统症状或诊断相关联的帧。对于解码分析主要要求对协议比较熟悉，这样才能看懂解析出来的报文。使用软件是简单的事情，能够利用软件解码分析来解决问题关键是要对各种层次的协议了解的比较透彻，工具软件只是提供一个辅助的手段。因为涉及的内容太多，这里不对协议进行过多讲解，请参阅其他相关资料。

在主机表选项卡中，采集了每个网络节点通信量的统计数据。对于 LAN，“主机表”选项卡包括 MAC 层、IP 网络层、IP 应用层、IPX 网络层和 IPX 传输层的信息，对于 WAN，“主机表”选项卡包括数据链路层、IP 网络层、IP 应用层、IPX 网络层和 IPX 传输层的信息。可以通过表、条形图或饼图查看累积数据。在所有的视图中，均可以显示数据链路层和 MAC 层的通信量或者选择性查看 IP 层或 IPX 层的通信量。

6）警报管理

Sniffer Pro 的警报功能提供了全面检测和记录网络警报事件的方法。专家系统在数据捕获过程中生成警报，当它检测到一个症状或诊断时，即会在警报日志中记录一次事件。监视功能的警报管理器将在 Sniffer Pro 启动后自动运行，一旦超过用户指定的阈值参数，它即会在警报日志中记录事件。通过“交换机统计数据”应用程序的“警报配置”选项卡，可以在不同的交换机端口上设置基于阈值的警报，一旦超过就向 Sniffer Pro 报警。警报可以分成 5 种不同的严重性级别：严重/诊断、主要、次要、警告和信息警报。警报日志中列出了所有警报事件，可通过选择监视菜单中的警报日志或者单击警报按钮显示该日志，如图 3-26 所示。

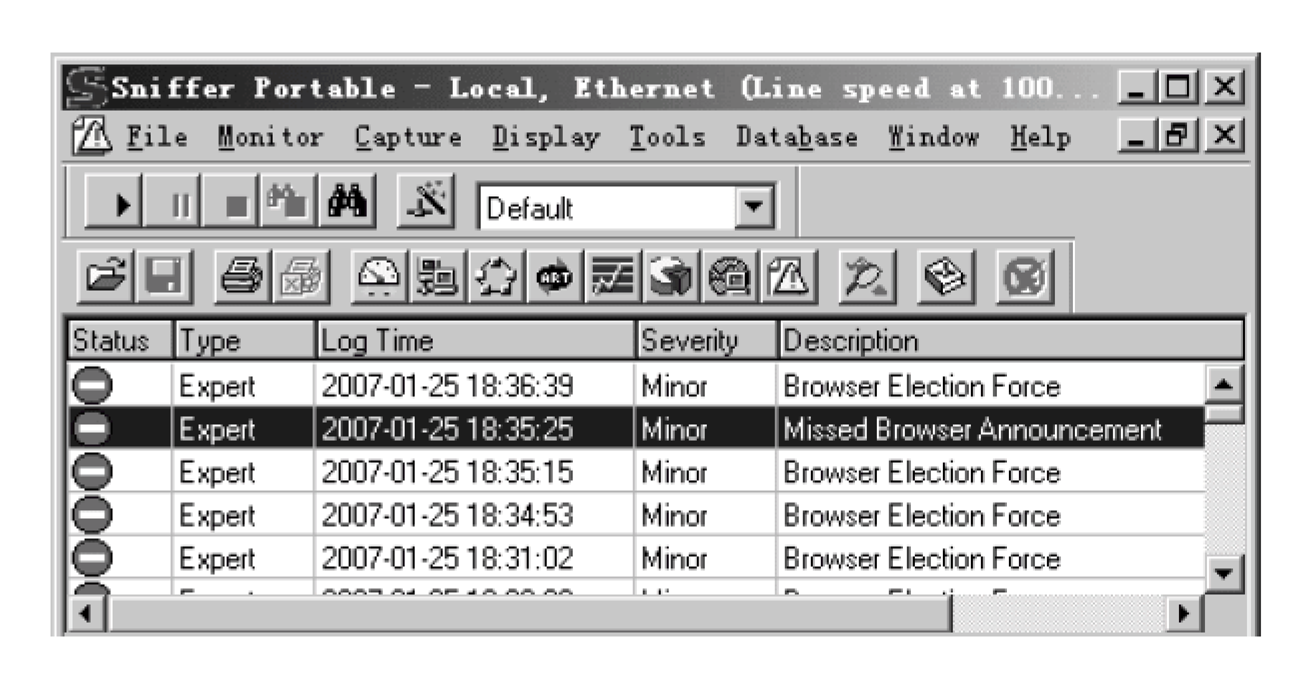



**图 3-26　警报日志**

7）Sniffer Pro 工具的使用

Sniffer Pro 提供了一组常用工具，可供标识和排除 IP 网络故障，这些工具包括 ping、Traceroute、DNS 查找、Finger 和 Whois，可以通过“工具”菜单来进行访问并使用。除了所提供的这组 Sniffer Pro 标准工具外，也可以在“工具”菜单中添加自己的工具，此工具可以是计算机上已安装用户计算机可以访问的任何 Windows 或 DoS 可执行文件，在添加新工具时，请指定启动该程序所需的路径、文件名和任何命令行参数，如图 3-27 所示。

此外，Sniffer Pro 还提供数据包生成器，利用它在网络中发送测试数据包，就可以重

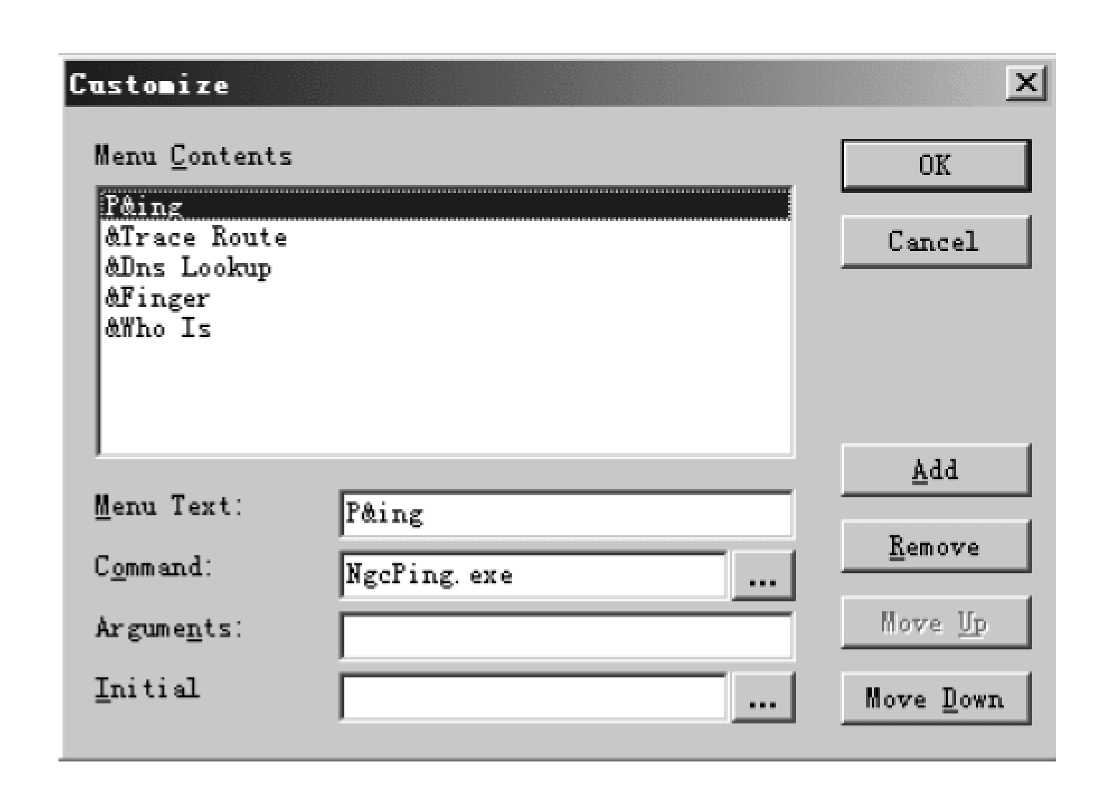



图 3-27 添加应用工具

现要排除的网络故障，验证对网络设备或应用程序的修复方法是否正确，也可以生成各级网络通信量负载，模拟实际的网络情况并对设备或应用程序进行测试。

### 2. EtherPeek NX

适用于 Windows 的 EtherPeek 是一种屡受嘉奖的以太网流量和协议分析器，EtherPeek 确立了“轻松使用”的行业标准。EtherPeek NX 是第一个提供信息包捕获过程中实时进行专业诊断和结构解码的网络协议分析器。EtherPeek NX 专门为 IT 人员设计，帮助分析和诊断日益加速变化的网络数据群。EtherPeek NX 是一款绿色软件，不用安装，也不需要加载额外协议的开销，运行速度快，系统资源占用小，去掉和隐藏了很多冗余的功能，功能简洁又不失强大。从其抓包和发包的一系列基本功能可以看出，操作方式上比 Sniffer Pro 更人性化。

1）系统安装

EtherPeek 对于不同的操作环境，极易安装与配置，使用自己的软件来绑定以太网卡。为更好体现其性能，工作环境最好具备 1GB RAM 或更多。大量捕获的包会存放在缓存里用以实时分析。EtherPeek 由 Alarm（报警）、Utilities（利用）、解码器（Packet decoders）、驱动器（Drivers）、Filters（过滤器）、分析模块（Analysis modules）等功能模块构成。系统安装结束后，就可以对数据包进行捕获了。在单击“开始抓包”按钮后，可以设置“抓包”选项，主要包括“常规”、“适配器”、“触发器”、“过滤器”、“输出形式”和“性能模块”，如图 3-28 所示。

可以对需要获取的包的类型进行设置，设定好包的类型后，就可以抓包了。单击“开始抓包”按钮，软件开始运行，同时对经过网卡的数据包进行捕获。

2）菜单与功能介绍

程序运行后，运行界面主要包括工具栏、主界面和状态栏三大块，如图 3-29 所示。工具栏包括“文件”、“编辑”、“查看”、“抓包”、“发送”、“监控”、“工具”、“窗口”与“帮助”9 个部分。

其基本的用法与其他 Sniffer 软件类似，为方便用户，在工具一栏中可以将一些应用工具加入到系统功能中，其中包括一些 Windows 系统自带的常用工具集，如图 3-30




图 3-28 抓包选项

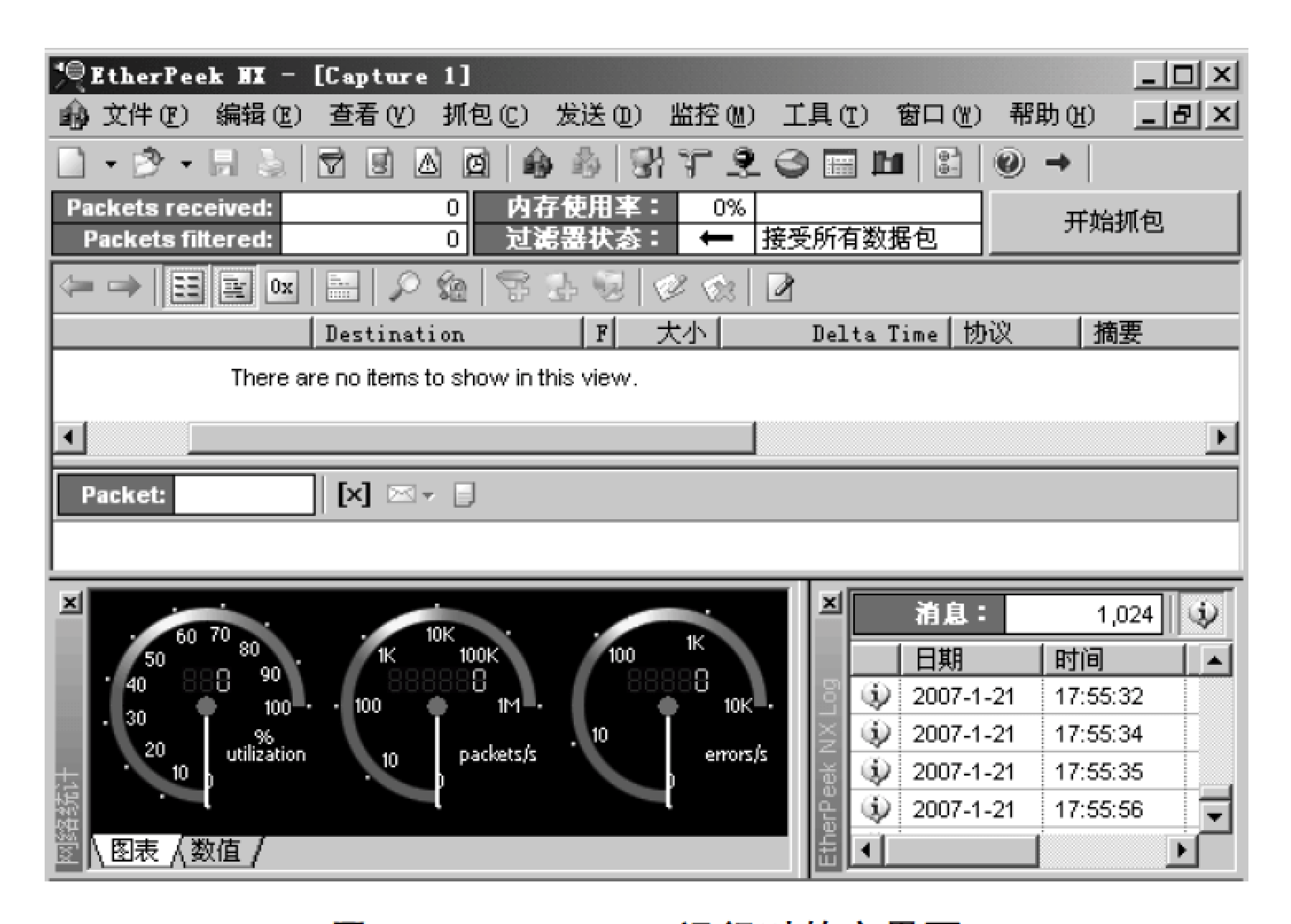



图 3-29 EtherPeek 运行时的主界面

所示。

3）如何捕获数据包

单击开始抓包，根据需求对数据包捕获一段时间后，就可以停止抓包了。EtherPeek 可以在多个不同配置的窗口对数据包进行捕获，每个窗口使用自己选取的适配器，使用自己的设置以及过滤规则，如图 3-31 所示。捕获窗口可以监视运行状况，选取统计信息，还可以实时监控网络流量，基于网络环境控制捕获动作，基于流量查看统计数据，查看捕获内容和进行解码，使用专家分析系统来监控和故障检测。捕获的数据包可以将其保存为 PKT、HTML 或其他形式的文件，以适合在不同的情况下查看。

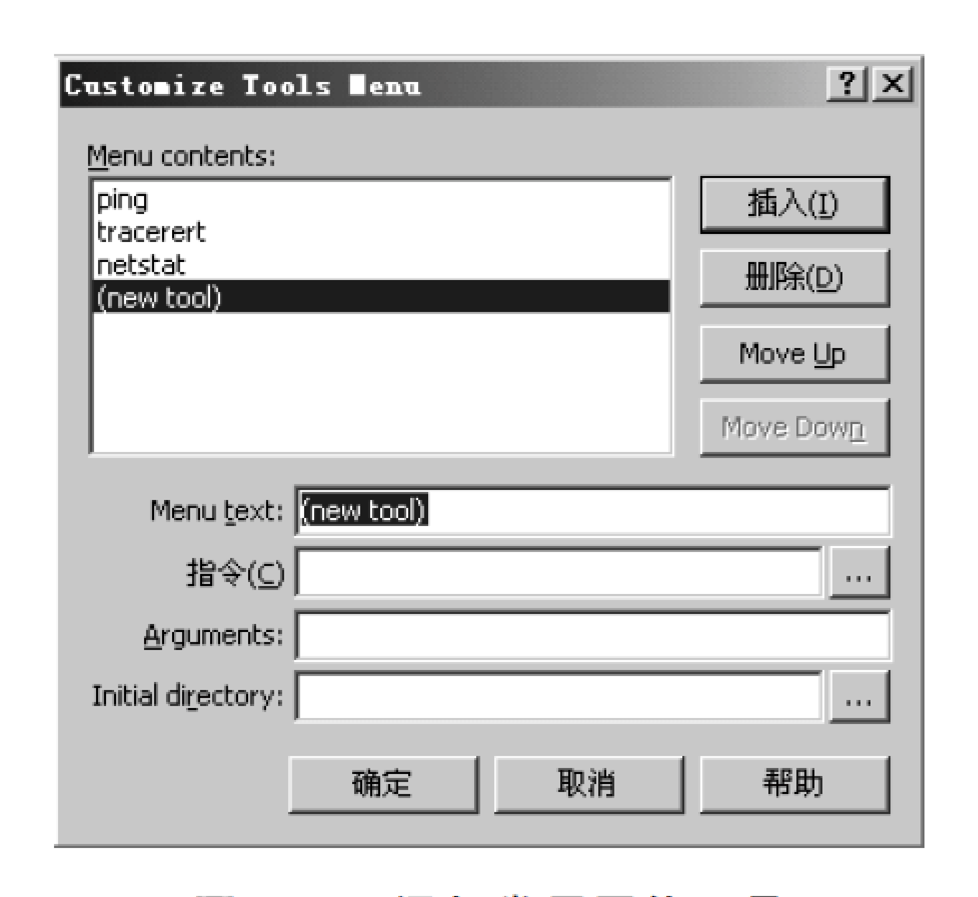



图 3-30　添加常用网络工具

EtherPee……，分析出潜在的网络安全问……件。可以根据自己的习惯配……了 91 个单独的事件，包括……此外还可以自己定义适合的……。专家系统不仅可以帮助分……示。

4）矩阵……

这些功能……料、主机间的通信联系、数……方法。

图 3-33　分析模块参数选择

5）分析模块

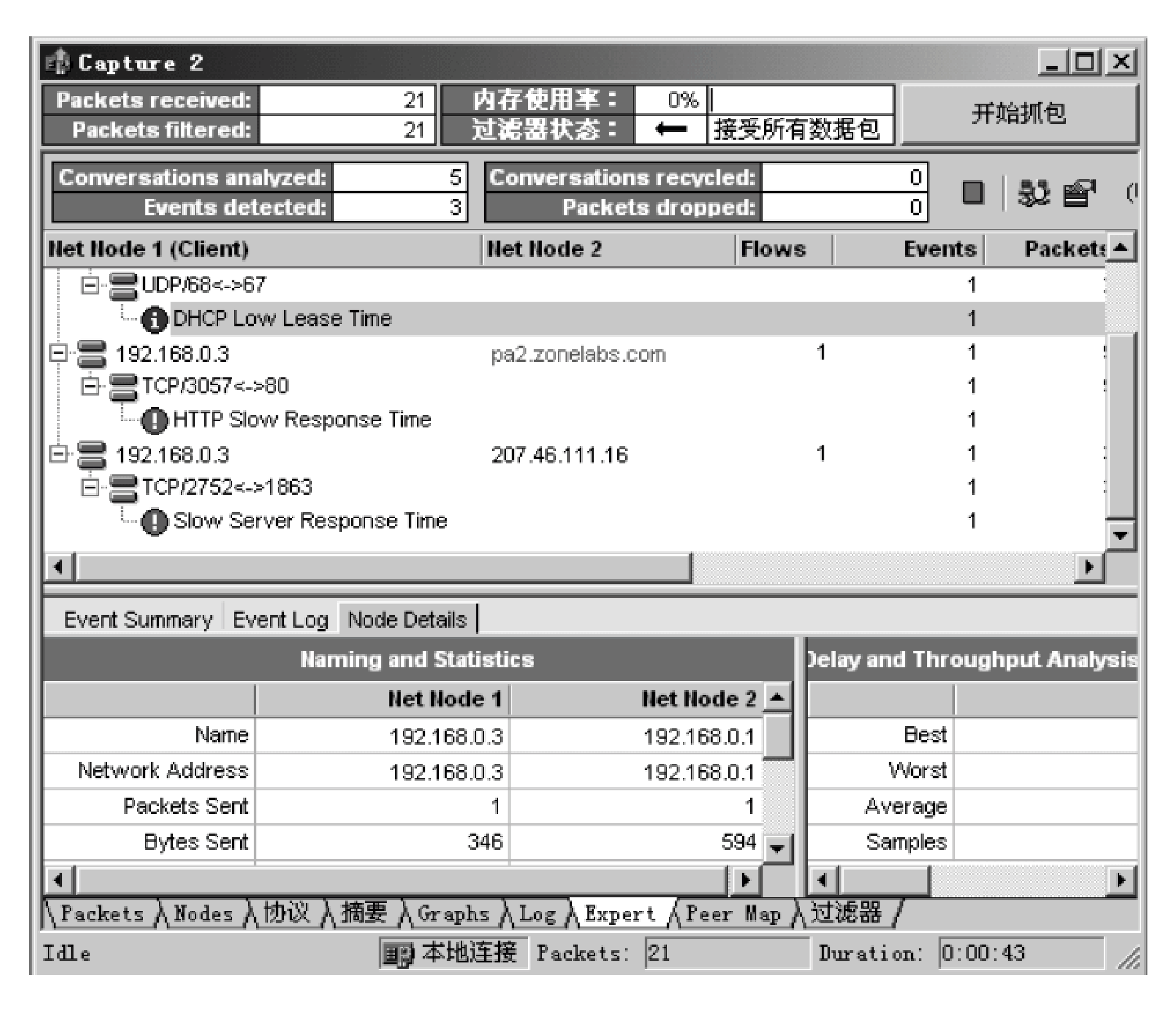



图 3-32 EtherPeek 的专家系统

分析模块是系统提供的外部高级特性，测试网络流量并提供详细的总结和特定流量计算的关键参数，并将结果提交到总结统计窗口。启用分析模块的功能适用于流量的实时捕获。可以单独启用或关闭这个功能。另外，许多分析模块需要自己进行配置。分析模块装载了大量常用的协议与网络应用，甚至可以自己编写分析模块。在启动分析模块时，可以选择相应的参数，如图 3-33 所示。分析模块集成了包括邮件分析模块、FTP 分析模块、ICMP 分析模块等常见应用层的应用，还包括一些网络攻击分析模块，如 IP 分析模块、RADIUS 分析模块、SQL 分析模块、VoIP 分析模块和 Web 分析模块等。当然还可以根据自己的需求，按照要求自己编写相应的分析模块。

6）数据包解码

作为一款好的网络监听软件，数据包解码的功能是必不可少的，EtherPeek 同样内置有解码工具，如图 3-34 所示。当检查网络的时候要对协议或安全漏洞进行分析，解码工具就很有用处了。具体的解码过程可以对照前面讲述的各种协议，进行细致深入的分析。

如果发现在网络里有 EtherPeek 不支持的特殊协议，或者开发了一个自己的协议，同样可以自己写一个解码器用在 EtherPeek 中。EtherPeek 允许用户写入自己的解码器，具体的编写方法可以参考相关资料。当然，这需要有相当的编程知识。

7）其他功能

EtherPeek 是一款优秀的网络监听工具，它还具有灵活的分布方式，可同时在多重网卡和多网络区段进行包捕捉。它可以支持一个单一程序 AcketGrabber 的远程分布，来实现多点分布式分析的功能，在远端只需要安装一个小的数据捕捉部分。还支持 Rmon 远程获取，这要由插件 RmonGrabber 来实现。EtherPeek NX 还具有丰富的功能插件群，能够直接转换几乎所有的网络分析软件捕获的数据包记录。

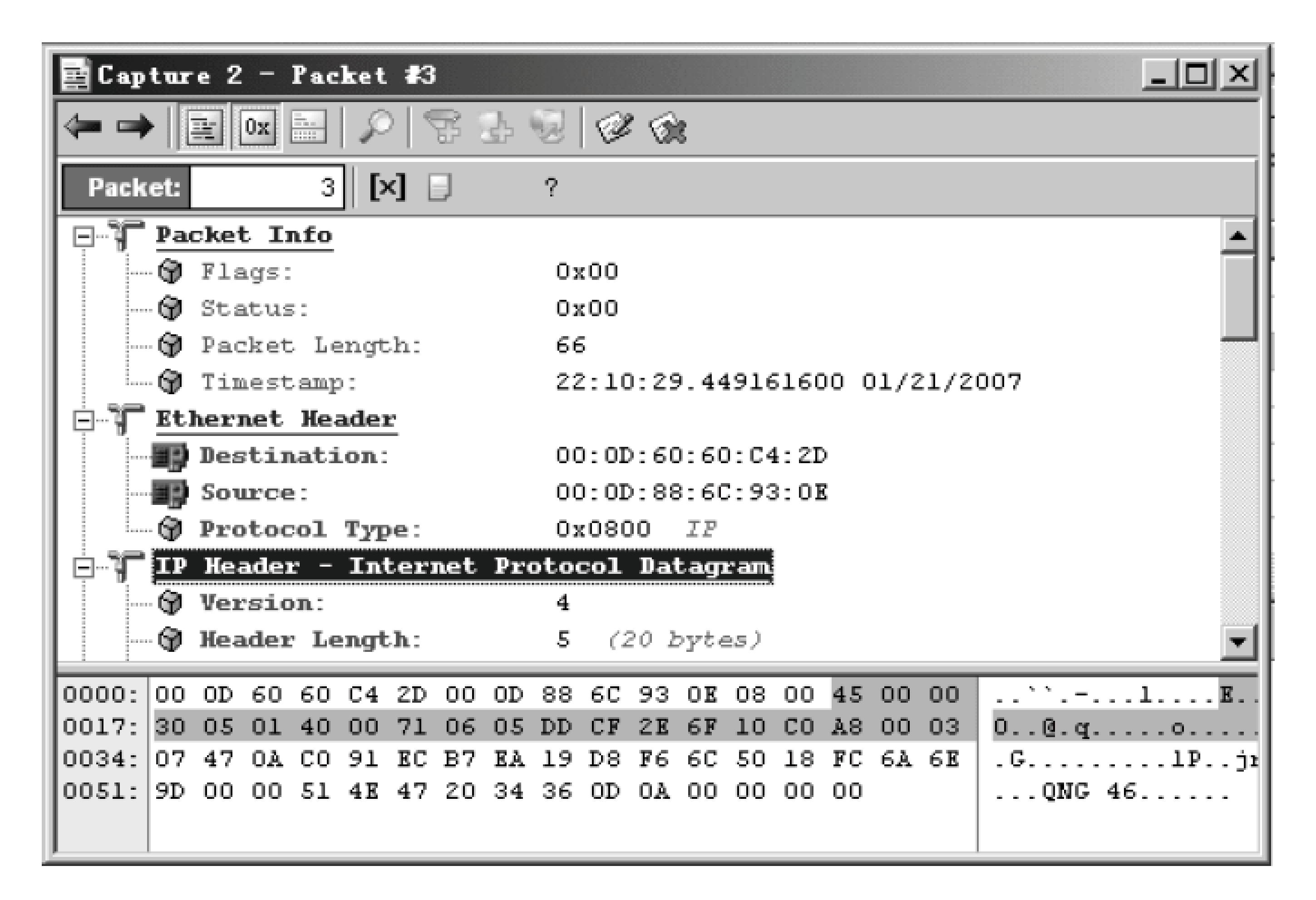



图 3-34　解码窗口

### 3. tcpdump

tcpdump 是 Linux/UNIX 系统下一个优秀的数据包监听软件。作为互联网上经典的系统管理员必备的工具，tcpdump 除了可以对网络上的数据包进行截获并加以分析外，还可以将网络中传送的数据包头截获下来提供分析，并支持针对网络层、协议、主机、网络或端口的过滤，提供 and、or、not 等逻辑语句来去掉无用的信息。而且由于 tcpdump 是一款基于 GNU 的免费的网络分析工具，提供了源代码，公开了接口，因此，它具备很强的可扩展性。tcpdump 以其强大的功能，灵活的截取策略，成为高级系统管理员分析网络、排查问题等所必备的工具之一。自其问世以来，一直受到管理员的青睐，得到了广泛的应用。

1）tcpdump 的安装

在 Linux 下 tcpdump 的安装十分简单，有些操作系统的发行包已经默认安装了这个工具。如果没有的话，一般可以采用两种安装方式，一种是以 rpm 包的形式来进行安装，另外一种是以源程序的形式安装。rpm 包的安装简单，通过 rpm 命令可以直接安装，不需要修改任何东西。Linux 的一个最大的诱人之处就是在它上面有很多软件是提供源程序的，管理员可以修改源程序来满足自己的特殊的需要，建议采取这种源程序的安装方法。

2）tcpdump 的应用

tcpdump 采用命令行方式，它的命令格式为：

```
tcpdump [-adeflnNOpqRStuvxX] [-c 数量] [-C 文件大小] [-F 文件名]
            [-i 网络接口] [-m 模块] [-r 文件名] [-s snaplen]
            [-T 类型] [-U 用户] [-w 文件名] [-E] [表达式]
```

其常用选项如下：

-a　将网络地址和广播地址转变成名字；

-d　将匹配信息包的代码以人们能够理解的汇编格式给出；

-dd 将匹配信息包的代码以C语言程序段的格式给出；

-ddd 将匹配信息包的代码以十进制的形式给出；

-e 在输出行打印出数据链路层的头部信息；

-f 将外部的Internet地址以数字的形式打印出来；

-l 使标准输出变为缓冲行形式；

-n 不把网络地址转换成名字；

-N 不打印域名；

-p 不将接口输出到混杂模式；

-q 快速输出，输出较少的协议信息；

-v 输出一个稍微详细的信息，例如，在IP包中可以包括TTL和服务类型的信息；

-vv 输出详细的报文信息；

-c 在收到指定数目的包后，tcpdump就会停止；

-F 从指定的文件中读取表达式，忽略其他的表达式；

-I 指定监听的网络接口；

-r 从指定的文件中读取包；

-w 直接将包写入文件中，并不分析和打印出来；

-T 将监听到的包直接解释为指定类型的报文，常见的类型有rpc和snmp。

3）tcpdump的表达式介绍

tcpdump的表达式是一个正则表达式，可以通过编写合适的表达式来进行报文过滤。如果一个报文满足表达式的条件，这个报文将会被相应的处理。如果没有给出任何条件，则所有的报文都将会被截获。在表达式中一般采用几种类型的关键字。一类是关于类型的关键字，主要包括host、net、port等，如“ host 192.168.1.2”表明192.168.1.2是一台主机，而“net 192.0.0.0”则指明192.0.0.0是一个网络地址，port 21指明端口号是21。如果没有指定类型，默认是host。第二类是确定传输方向的关键字，主要包括src、dst、dst or src，dst and src等，这些关键字指明了传输的方向。比如，“src 192.168.1.2”指明IP包中源地址是192.168.1.2，“dst net 192.0.0.0”指明目的网络地址是192.0.0.0。如果没有指明方向关键字，则默认是src or dst关键字。第三类是协议的关键字，主要包括ip、arp、rarp、tcp、udp等类型，用它来指明监听的包的协议内容。如果没有指定任何协议，tcpdump将会监听所有协议的信息包。除了这三种类型的关键字之外，其他重要的关键字还包括gateway、broadcast、less、greater以及三种逻辑运算。取非运算是not或!，与运算是and或&&，或运算是or或||。系统管理员可以将这些关键字组合起来构成强大的逻辑关系，以满足网络检测的需求。

4）tcpdump的输出结果介绍

tcpdump具有强大的功能，输出的信息量很大，有必要对其输出的信息进行分检与过滤。首先，介绍几种典型的tcpdump命令的输出信息，便于读者理解。

Tcpdump的输出格式有以下几种。

（1）UDP数据包

```
15:22:41.400299 test.test.edu.cn.1052 > 192.168.1.3.57392: udp 110
```

时间戳：15:22:41.400299

源地址：test.test.edu.cn

源端口：1052

目的地址：192.168.1.3

目的端口：57392

协议：udp

大小：110

（2）TCP 数据包

```
16:23:01.079553 test.test.edu.cn.33635 > target.test.edu.cn.32772: P 12765:12925(160) ack 19829 win
24820 (DF)
```

时间戳：16:23:01.079553

源地址：test.test.edu.cn

源端口：33635

目的地址：target.test.edu.cn

目的端口：32772

表明 PUSH flag 设为 P

序列号：12765：

从序列号开始到 12925 所包括的字节数，但不包括 12925

用户数据包字节数：(160)

窗口大小：24820

ack 号：19829

要 tcpdump 显示的详细信息，包括显示每个数据包的详细信息，可以使用下面的参数。

```
tcpdump -v <expression>
tcpdump -vv <expression>
tcpdump -vvv <expression>
```

5）tcpdump 的具体使用

tcpdump 支持许多参数，如使用-i 参数来指定监听的网络适配器，在计算机具有多个网络适配器时非常有用；使用-c 参数指定要监听的数据包数量；使用-w 参数指定将监听到的数据包写入文件中保存等。

因为网络中数据流量很大，虽然网络分析工具能将这些传送的数据记录下来，但如果不加分辨就将所有的数据包都截留下来的话，由于数据量过于庞大，反而不容易发现需要的数据包。所以 tcpdump 采用参数来进行数据包过滤，使用这些参数定义的过滤规则可以截留特定的数据包，缩小目标范围，以便更好的分析网络中存在的问题。这些参数指定要监视数据包的类型、地址、端口等。根据具体的网络问题，充分利用这些过滤规则就能达到迅速定位故障的目的。

从上面 tcpdump 的输出可以看出，tcpdump 对截获的数据并没有进行彻底解码，数

据包内的大部分内容是使用十六进制的形式直接打印输出的。这显然不利于分析网络故障,通常的解决办法是先使用-w 参数截获数据并保存到文件中,然后再使用其他程序进行解码分析。当然也应该定义过滤规则,以避免捕获的数据包填满整个硬盘。

不带任何参数的 tcpdump 将搜索系统中所有的网络接口,并显示它截获的所有数据。这些数据不一定全都需要,而且数据太多不利于分析。所以,应当先想好需要哪些数据,以下参数可以为选择数据提供参考。

-b 在数据链路层上选择协议,包括 ip、arp、rarp、ipx 都是这一层的。

例如:

```
[root@ test root]#tcpdump   arp
```

将只显示网络中的 arp 即地址转换协议信息。

如果是作为路由器至少有两个网络接口,通过-i 这个选项来选择网络接口。例如:

```
[root@ test root]#tcpdump -i eth0
```

只显示通过 eth0 接口上的所有报头。

src、dst、port、host、net、ether、gateway 这几个选项又分别包含 src、dst、port、host、net、ehost 等附加选项,用来分辨数据包的源地址和目的地址,如“src host 192.168.0.1”指定源主机 IP 地址是 192.168.0.1,“dst net 192.168.0.0/24”指定目标是网络 192.168.0.0。以此类推,host 是与其指定主机相关,无论它是源还是目的,net 是与其指定网络相关的,ether 后面跟的不是 IP 地址而是物理地址,而 gateway 则用于网关主机。

```
[root@ test root]#tcpdump src host 192.168.0.1 and dst net 192.168.0.0/24
```

表示过滤的是源主机为 192.168.0.1 与目的网络为 192.168.0.0 的报头。

```
[root@ test root]# tcpdump src host 192.168.0.1 and dst port not telnet
```

表示过滤源主机 192.168.0.1 和目的端口不是 Telnet 的报头。

ip、icmp、arp、rarp 和 tcp、udp、icmp 等这些选项都要放到第一个参数的位置,用来过滤数据报的类型。例如:

```
[root@ test root]tcpdump ip src net 192.168.0.0
```

表示只过滤网络 192.168.0.0 数据链路层上的 IP 报头。

```
[root@ test root]tcpdump udp and src host 192.168.0.1
```

表示只过滤源主机 192.168.0.1 的所有 udp 报头。

#### 4. 网络监听的检测与防范

网络监听技术作为一种工具,总是扮演着正反两方面的角色。对于入侵者来说,最喜欢的莫过于用户的密码,通过网络监听可以很容易地获得这些关键信息。而对于入侵检测和追踪者来说,网络监听技术又能够在与入侵者的斗争中发挥重要的作用。由于运行网络监听的主机只是被动地接收在局域网上传输的信息,它并不主动的与其他主机交

换信息,也不修改在网上传输的数据包,所以网络监听是很难被发现的,但是可以通过一些方法,利用一些常用的简单工具,对是否存在网络监听进行初步简单的判断。

1)较高的通信丢包率

通过一些网管软件,可以看到数据包传送情况,最简单是 ping 命令,它会告诉用户丢掉了百分之多少的数据包。如果网络结构正常,在排除病毒的影响外,如果有 20%～30%数据包丢失,以致数据包无法顺畅的到达目的地,网络被监听的可能性较大,可能是由于嗅探器拦截数据包而导致。

2)网络带宽出现异常

通过某些带宽控制器,可以实时看到目前网络带宽的分布情况,如果某台机器长时间的占用了较大的带宽,这台机器就有可能在实施网络监听。由于监听程序要分析和处理大量的数据包会占用很多的 CPU 资源,如果某台机器服务性能下降,也应该可以察觉出网络通信速度的变化。

鉴于目前的网络安全现状,应该进一步了解与学习网络监听技术的细节,从技术基础上掌握先机,才能在与入侵者的斗争中取得胜利。为了安全起见,非网络管理用途的计算机上不应该运行网络分析软件。当网卡被设置为混杂模式时,系统会在控制台和日志文件中留下记录,需要留意这台系统是否被用作攻击同网络的其他计算机的跳板。对网络监听的防范可以从以下几个方面采取措施。

(1)采用安全的拓扑结构。对于以太网而言,Sniffer 只能在当前网段上进行数据捕获。因此交换机、路由器和网桥三种网络设备是 Sniffer 不能跨过的,用户可以通过运用这些设备来进行网络分段,将网络分段工作进行的越细,嗅探器能够收集的信息就越少。由于大多数早期建立的内部网络都使用 HUB(集线器)来连接多台工作站,当用户与主机进行数据通信时,两台机器之间的数据包(称为单播包 Unicast Packet)会被同一台集线器上的其他用户所监听。所以有条件的话,应该以交换机代替共享式集线器,使单播包仅在两个节点之间传送,从而防止非法监听。

(2)采用加密技术。数据经过加密后,尽管通过监听仍然可以得到传送的信息,但显示的是经加密过的信息,而这些数据是没有用的。使用加密技术的缺点是影响数据传输速度且使用弱加密算法比较容易被攻破。所以系统管理员和用户需要在网络速度和安全性上进行折中,由于目前网络传输的速度并不是一个严重的问题,所以应尽可能地采用加密技术。在加密时有两个主要的问题,一个是技术问题,一个是人为问题。技术是指加密能力是否高,例如,使用 64 位加密就可能不够,而且并不是所有的应用程序都集成了加密支持。目前跨平台的加密方案还比较少见,一般只在一些特殊的应用之中才有。人为问题是指有些用户不喜欢加密,觉得过于麻烦。传统的网络服务程序,如 SMTP、HTTP、FTP、POP3 和 Telnet 等在本质上都是不安全的,因为它们在网络上用明文传送密码和数据,Sniffer 非常容易就可以截获这些密码和数据,必须用一种更好的应用程序来代替,如使用 secure shell、secure copy 或者 IPv6 协议都可以使得信息安全的传输。SSH(secure shell)程序可以通过网络登录到远程主机并执行命令,其绑定在端口 22 上,连接采用协商方式使用 RSA 加密,身份鉴别完成之后,后面的所有流量都使用 IDEA 进行加密。SSH 的加密隧道保护的只是中间传输的安全性,它提供了很强的安全验证可

以在不安全的网络中进行安全的通信，使得任何通常的Sniffer工具软件无法获取发送的内容。可以通过使用SSH把所有传输的数据进行加密，这样“中间服务器”这种攻击方式就不可能实现了，而且也能够防止DNS和IP欺骗。还有一个额外的好处就是传输的数据是经过压缩的，所以可以加快传输的速度。SSH有很多功能，它既可以代替Telnet，又可以为FTP、POP，甚至PPP提供一个安全的“通道”。

(3) 用静态的ARP或者IP-MAC对应表代替动态的ARP或者IP-MAC对应表。该措施主要是进行渗透Sniffer的防范，采用诸如ARP欺骗手段能够让入侵者在交换网络中顺利完成嗅探。Sniffer中通常使用的ARP欺骗，主要是通过欺骗进行ARP动态缓存表的修改。可以在重要的主机或者工作站上设置静态的ARP对应表，比如，在Win2K系统中可以使用arp命令进行设置，在交换机上可以设置静态的IP-MAC对应表等，来防止入侵者利用欺骗手段进行Sniffer。

除了以上三点，另外还要重视重点区域的安全防范。这里说的重点区域，主要是针对Sniffer的放置位置而言。入侵者要让Sniffer发挥较大功效，通常会把它设置在数据交汇集中区域，比如网关、交换机、路由器等附近，以便能够捕获更多的数据。因此，对于这些区域就应该加强防范，防止在这些区域存在嗅探器。另外，对于网络的安全，管理显得格外重要。除系统管理员外其他人员禁止在网络中使用任何的Sniffer工具，包括一些企业高级管理人员，从制度上明确限制一些工作站主动使用Sniffer工具。

对于系统管理员来说更重要的是要建立安全意识，了解你的用户、定期检查网络中的重点设备(如服务器、交换机、路由器)。如果确信有人接了Sniffer到网络上，可以去找一些进行验证的工具，这种工具称为时域反射计量器(Time Domaio Reflectometer，TDR)。TDR会对电磁波的传播和变化进行测量，将一个TDR连接到网络上，能够检测到未授权的获取网络数据的设备。系统管理员还需要给用户提供安全服务，定期发送安全邮件或发布安全公告，让用户具有安全意识。管理意识是提高安全性的另一个重要因素，管理部门需要根据安全策略，建立一套每个人都必须遵守的安全标准。如果系统管理员在此基础再建立自己的安全规则，就强化了安全。此外系统管理员不仅仅需要从技术上考虑问题，还要站在用户的观点上考虑问题，提供一些提高安全的工具，使安全保护方法对用户尽可能地简单，这样也便于用户接受，从另一个方面也减轻了系统管理员的安全压力。

## 3.4 路由器安全策略

路由器是互联网的主要节点设备，它构成了Internet的骨架，是网络中最基础、重要的网络设备。路由器决定数据的转发，直接影响着网络互联的质量，有效的路由器配置可以提高网络的安全性。思科系统公司是全球领先的互联网设备供应商，提供业界范围最广的网络硬件产品、互联网操作系统(IOS)软件、网络设计和实施等专业技术支持，其路由器技术最为权威，是行业公认的业界标准。这里选用Cisco路由器来举例说明其在网络安全中的作用。Cisco路由器的功能是通过适当的IOS命令来实现的，因此对路由器的操作也就是对IOS相关命令的正确使用。有关IOS的基本命令可以参考相关资料，这里重点讲述其对于网络安全方面的功能及操作。

## 3.4.1 路由器访问安全配置

由于路由器出厂时，常常设定了一些默认的密码及服务，如果黑客能够浏览系统的配置文件，就会引起身份危机，所以建议启用路由器上的密码加密功能，同时需要管理员禁用一些不必要的服务。另外，要实施合理的验证控制以便路由器安全地传输证书，可以配置一些协议(如远程验证拨入用户服务)，这样就能使用这些协议结合验证服务器提供经过加密验证的路由访问。验证控制可以将用户的验证请求转发给通常在后端网络上的验证服务器。验证服务器可以要求用户使用双因素验证，以此加强验证系统。双因素的前者是软件或硬件的令牌生成部分，后者则是用户身份和令牌通行码。其他的验证解决方案涉及在安全外壳(SSH)或 IPSec 内传送安全证书，具体的配置方法是禁用 enable password 命令，而采用 enable secret 命令设置密码，该加密机制是 IOS 采用 MD5 散列算法进行加密。

```
Router(config-t)#enable secret
Router(config-t)#no enable password
Router(config-t)#service password-encryption
Router(config-t)#line vty 0 4
Router(config-line)#exec-timeout 10 0
```

或者使用基于用户名和密码的强认证方法

```
Router(config-t)#username admin pass 5 434535e2
Router(config-t)#aaa new-model
Router(config-t)#RADIUS-server host 110.1.1.1 key key-string
Router(config-t)#aaa authentication login netadmin group RADIUS local
Router(config-t)#line vty 0 4
Router(config-line)#login authen netadmin
```

## 3.4.2 路由器服务安全管理

路由器操作系统和网络操作系统一样容易受到黑客的攻击，但大多数中小企业都没有雇佣路由器工程师，也没有把这项工作当成一件必须要做的事情外包出去。因为网络管理员和经理人并不十分了解保证路由器安全的重要性。下面是保证路由器安全的一些基本技巧。

**1. 更新路由器操作系统**

就像网络操作系统一样，路由器操作系统也需要更新，以便纠正编程错误、软件瑕疵和缓存溢出的问题。要经常向路由器厂商查询当前的更新和操作系统的版本。

**2. 修改默认的密码**

据卡内基梅隆大学的计算机应急反应小组称，80%的安全事件都是由于较弱或者默

认的密码引起的。应避免使用普通的密码,并且使用更强大的密码规则,如大小写字母混合的方式。

### 3. 关闭 CDP 服务

系统默认启动 Cisco 发现协议(Cisco discovery protocol,CDP),它是一种独立媒体协议,运行在所有思科本身制造的设备上。其主要功能是用来获取相邻设备的协议地址以及发现这些设备的平台,缺陷是会对所有发出的设备请求做出应答,能发现邻近的 Cisco 设备、型号和软件版本,有可能威胁到路由器的安全,并产生额外的系统负担,应尽量禁止其运行。管理员也可以输入以下接口命令禁止某端口的 CDP。

```
Router(config-t)#no cdp run
Router(config-t)#int s0
Router(config-if)#no cdp enable
```

### 4. 禁用 HTTP 设置和 SNMP

Cisco 路由器一般允许使用 Web 界面来进行配置,这样可以为管理员的管理提供方便,但也带来了许多隐患。如果没有特别的需要,最好关闭这个服务。如果启用了 HTTP 服务则需要对其进行安全配置,设置用户名和密码,采用访问列表进行控制。下面是一个简单的标准访问控制列表配合使用 HTTP 服务的示例。

```
Router(Config)#username manage privilege 10 G00dPa55w0rd
Router(Config)#ip http auth local
Router(Config)#no access-list 10
Router(Config)#access-list 10 permit 192.168.0.1
Router(Config)#access-list 10 deny any
Router(Config)#ip http access-class 10
Router(Config)#ip http server
```

如果没有使用路由器上的 SNMP,那么就不需要启用这个功能。思科路由器存在一个容易遭受 CRE 隧道攻击的 SNMP 安全漏洞。

### 5. VTY 的服务控制

VTY 是 Telnet 虚拟终端,管理员可通过其远程管理设备。如果想成功登录到设备,必须在 line 线路下使用命令 password 来定义登录密码;否则无法成功登录。在此配置的密码是保存在配置文件中的,即使启用 service password-encryption 功能,其加密的方式也是一种可逆的加密,很容易破解,所以在使用过程中尽可能配置一个不同于特权模式的密码。在 line vty 线路中,默认情况下使用的是系统默认的登录方式,如果需要在登录时指定认证模式,可以使用 login authentication 命令进行指定。通过 VTY 线路登录后,会进入用户模式,如果需要进行特权模式,那么必须配置登录特权模式的认证。不应该将它处于随意登录状态,假如只允许 192.168.0.3 这台主机能够用 Telnet 访问设备,需做如下设定。

```
Router(config-t)#access-list 110 permit ip 192.168.0.3 0.0.0.0 192.168.0.2 0.0.0.0 log
Router(config-t)#line vty 0 4
Router(config-t)#access-class 101 in
Router(config-t)#exec-timeout 5 0
```

### 6. 其他需要关闭的服务

永远禁用不必要的服务无论是路由器、服务器和工作站上的都要禁用。Cisco 路由器功能强大，通过网络操作系统默认地提供了一些小的服务，如 echo(回波)、chargen(字符发生器协议)和 discard(抛弃协议)。在配置一个路由器时，需要遵循最小化原则，也就是只开放必要的服务，这样可以有效地保证路由器的安全，防止对于路由器的 DDoS 攻击，节省内存并防止安全破坏行为。一些常见的需关闭的服务有。

```
Router(config-t)#no service finger
Router(config-t)#no service pad
Router(config-t)#no service udp-small-servers
Router(config-t)#no service tcp-small-servers
Router(config-t)#no ip http server
Router(config-t)#no service ftp
Router(config-t)#no ip bootp server
```

### 7. 封锁 ICMP(互联网控制消息协议)ping 请求

ping 和其他 ICMP 功能对于网络管理员和黑客都是非常有用的工具。黑客能够利用路由器上启用的 ICMP 功能找出可用来攻击网络信息。为了防止 ICMP-flooging 攻击，还需在相应的端口下关闭以下服务。

```
Router(config-t)#int e0
Router(config-if)#no ip redirects
Router(config-if)#no ip directed-broadcast
Router(config-if)#no ip proxy-arp
```

### 8. 禁用来自互联网的 Telnet 命令

在大多数情况下，不需要来自互联网接口的主动 Telnet 会话，如果从内部访问路由器设置会更安全一些。

### 9. 禁用 IP 定向广播

IP 定向广播能够允许对设备实施拒绝服务攻击。一台路由器的内存和 CPU 难以承受太多的请求，这种结果会导致缓存溢出。

### 10. 禁用 IP 路由和 IP 重新定向

重新定向允许数据包从一个接口进来然后从另一个接口出去，不需要把精心设计的

数据包重新定向到专用的内部网路。

**11. 包过滤**

包过滤仅传递允许进入网络的那种数据包。许多公司仅允许使用80端口(HTTP)和110/25端口(电子邮件)。此外还可以封锁和允许IP地址和范围。

**12. 审查安全记录**

通过简单地利用一些时间审查记录文件,会看到明显的攻击方式甚至安全漏洞,而且会为经历了如此多的攻击感到惊奇。

### 3.4.3 其他相关安全问题

**1. 系统漏洞问题**

和操作系统及其他软件一样,路由器自己的操作系统即网络操作系统(IOS)也会出现漏洞及安全隐患,需要管理员及时关注产品信息打上安全补丁,同时认真严格的为IOS作安全备份,这样可以大大减少路由器漏洞问题的发生。

**2. 访问控制问题**

要做好以下两个方面的限制,一是限制系统物理访问;二是限制逻辑访问。限制系统物理访问是确保路由器安全的有效方法。限制系统物理访问就是要避免将调制解调器连接至路由器的辅助端口,或者将控制台和终端会话配置成在较短闲置时间后自动退出系统。限制逻辑访问主要是借助于访问控制列表,由于访问控制列表在数据过滤方面的重要作用,所以下面单列一段对此进行详细阐述。

**3. 路由协议问题**

在路由协议方面,要避免使用路由信息协议(RIP),因为RIP很容易被欺骗从而接受不合法的路由更新。最好是各个分支机构都统一配置,使用开放最短路径优先协议(OSPF),以便在接受路由更新之前,通过发送密码的MD5散列,使用密码验证对方。

**4. 配置管理问题**

要有控制存放、检索及更新路由器配置的配置管理策略,将配置备份文档妥善保存在安全服务器上,以防新配置遇到问题时方便更换、重装或恢复到原先的配置。可以通过两种方法将配置文档(包括系统日志)存放在支持命令行接口(CLI)的路由器平台上。一种方法是运行脚本,使其能够在服务器到路由器之间建立SSH会话、登录系统、关闭控制器日志功能、显示配置、保存配置到本地文件以及退出系统。另外一种方法是在服务器到路由器之间建立IPSec隧道,通过该安全隧道内的TFTP将配置文件复制到服务器。

## 3.4.4 访问控制列表的制定

使用访问控制列表的目的就是为了保护路由器的安全和优化网络的流量。访问列表的作用就是在数据包经过路由器某一个端口时,该数据包是否允许转发通过,必须先在访问控制列表里边查找,如果允许则给予通过。访问列表有多种形式,主要有标准ACL、扩展ACL和命名ACL等。

### 1. 标准ACL

通过使用IP包中的源IP地址进行过滤,一个标准访问控制列表的基本配置如下所示。

```
access-list access-list-number {deny|permit} source [source-wildcard]
```

其中access-list-number是定义访问列表编号的一个值,范围从1～99或1300～1999,参数deny或permit指定了允许还是拒绝数据包参数,source是发送数据包的主机地址,source-wildcard则是发送数据包的主机的通配符。在实际应用中,如果数据包的源地址在访问列表中未能找到或是找到了未被允许转发,则该包将会被拒绝。配置了访问列表后,就要启用访问控制列表,需要在接口配置模式下使用access-group或ip access-class命令来指定访问列表应用于某个接口。使用关键字in或out来定义该接口是出站数据包还是入站数据包。

### 2. 扩展ACL

由于标准访问控制列表对使用的端口不进行区别,所以引入了扩展访问控制列表。

扩展访问列表能够对数据包的源地址、目的地址和端口等项目进行检查,它比标准ACL具有更多的匹配选项,功能更加强大和细化,可以针对包括协议类型、源地址、目的地址、源端口、目的端口和TCP连接等进行过滤,表号范围是100～199或2000～2699。这其中,任何一个项目都可以导致某个数据包不被允许经过路由器接口。简单的配置过程如下。

```
Router #configure t
Router(config)#ip access-list extended 101
Router(config-ext-nacl)#permit tcp any host 10.1.1.2 established log
Router(config-ext-nacl)#permit tcp any host 10.1.1.2 eq www log
Router(config-ext-nacl)#permit tcp any host 10.1.1.2 eq ftp log
Router(config-ext-nacl)#permit tcp any host 10.1.1.2 log
```

经过上述配置,形成如下的访问列表。

```
access-list 101 permit tcp any host 10.1.1.2 established log
access-list 101 permit tcp any host 10.1.1.2 eq www log
access-list 101 permit tcp any host 10.1.1.2 eq telnet log
access-list 101 permit tcp any host 10.1.1.2 log
```

第一行允许通过TCP协议访问主机10.1.1.2,如果某个连接已经在主机10.1.1.2

和某个要访问的远程主机之间建立,则该行不会允许任何数据包通过路由器接口,除非会话是从内部企业网内部发起的。第二行允许任何连接到主机 10.1.1.2 来请求 www 服务,而所有其他类型的连接将被拒绝,这是因为在访问列表中会默认的在列表尾部加上一个 deny any any 语句来限制其他类型连接。第三行是拒绝任何 telnet 连接来访问 10.1.1.2 主机。第四行是允许所有类型的访问连接到 10.1.1.2 主机。把这个 ACL 定义到相应的接口上,就可以完成相应的控制功能。

Cisco 路由器新增加了一种基于时间的访问控制列表。这种基于时间的访问控制列表是在原来的标准访问控制列表和扩展访问控制列表中,加入有效的时间范围来更合理有效地控制网络。先定义一个时间范围,然后在原来的各种访问控制列表的基础上应用它。通过它,可以根据一天中的不同时间、一星期中的不同日期或者结合两者来控制网络数据包的转发。合理配置基于时间的访问控制列表可以更有效地保护内部网络,降低网络被攻击的几率。一个简单的基于时间 ACL 的例子如下。

```
Router #configure t
Router(config-t)#time-range Test
Router (config-time-range)#periodic weekdays 7:00 to 19:00
Router(config-t)#ip access-list extended 101
Router(config-ext-nacl)#permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range Test
```

这个基于时间的访问列表起的作用就是在每天 7:00 至 19:00,允许 Telnet 的网络流量。

### 3.4.5 使用路由器 ACL 保护网络

通过上述 ACL 的说明,了解了 ACL 的作用。利用路由器来保护局域网络,本质上也就是采用一系列访问控制命令来对网络数据流进行管理。通过设置类似于源地址、目的地址、端口号、协议等特定指示条件来指示路由器哪些数据包可以接收、哪些数据包需要拒绝。建立访问控制列表后,可以限制网络流量,提高网络性能,对通信流量起到控制的手段,减少被攻击的风险,这也是保护局域网络安全的基本手段。下面详细说明如何利用 ACL 对局域网络进行安全控制。

#### 1. 过滤 TCP 协议

如果一个局域网需要为用户提供的主要网络应用有远程登录访问(Telnet)、发送接收电子邮件(SMTP 和 POP3)、主页浏览(HTTP)等,要求局域网用户可以任意访问其他网络。那么路由器的访问控制列表可以定义如下。

```
access-list 100 permit tcp any 192.168.18.0 0.0.0 255 eq 23
access-list 100 permit tcp any 192.168.18.0 0.0.0.255 eq 25
access-list 100 permit tcp any 192.168.18.0 0.0.0.255 eq 110
access-list 100 permit tcp any 192.168.18.0 0.0.0.255 eq 80
access-list 100 permit tcp any any established
interfaces eria 10
```

```
ip access-group 100 in
```

需要注意的是，在建立访问控制列表一段时间后，可以使用命令 show access-list 100 来检查每项 ACL 后面括号中 TCP 报文的 matched 数量，根据 matched 数量由大到小的顺序重新排列访问控制列表的控制顺序，这样可以减少报文在访问控制列表中不必要的检测，减少特定报文查找访问控制列表的时间，降低路由器 CPU 的负担。另外，注意在 access-list 100 的最末尾使用关键字 established。使用关键字 established 是一种判断报文是否为一个已知会话一部分的简单方法，它被 Cisco 路由器访问控制列表用来允许 TCP 返回的报文。它检测 TCP 报文中 ACK 或 RST 标志位的存在，如果报文中的 ACK 或 RST 位被设置了，则通常表示报文是一个正在进行的会话的一部分。但入侵者可以编写程序，用来生成这两个标志，并将带有 ACK 或 RST 标志位的报文发送出去，而这些报文却并非正在进行的合法会话的一部分。由于 TCP 返回的报文随机选择的端口号范围是 1024～65536，所以可以将含有关键字 established 的访问控制语句改为“access-list 100 permit tcp any 192.168.18.0 0.0.0.255 gt 1023 established”，这就确保了进入企业内部网络的报文目的端口号都大于 1023，如果入侵者企图逃脱访问控制列表项的控制使用 ACK 和 RST 位，那么它的端口号必须大于 1023，这就使得欺骗性的报文不会对端口号低于 1024 的服务造成影响，在一定程度上提高了网络的安全性。

#### 2. 过滤 UDP 协议

UDP 协议和 TCP 协议的区别在于 UDP 是一种无连接的协议，其不会有 SYN-ACK 协商。因此，UDP 报文头也不存在类似 TCP 协议 ACK 位或 RST 位那种可以确定某个报文是否为一个已存在会话一部分的位。由于网络上利用 Windows 系统 NetBIOS 漏洞(UDP port 137-139)进行攻击的程序很多，所以必须对这部分 UDP 协议进行过滤，以防止局域网络的计算机系统被攻击，同时也不能影响 WINS 的名字解析工作。如果提供服务的网络操作系统是基于 Windows NT 平台的，使用 WINS 服务器解析计算机名，而 WINS 服务器不在企业总部而在分支机构，IP 地址为 192.168.2.245，假设端口为 137，根据客户机的端口号是在 1023 以上随机选择的这样一个规则，使用如下命令来抵制利用 NetBIOS 漏洞发起的攻击。

```
access-list 100 permit udp 192.168.2.245 0.0.0 0 eq 137 any gt 1023
```

虽然入侵者可以在分支机构欺骗性地使用源地址和源端口发送类似 WINS 服务器的报文，但是由于企业总部服务器的端口通常小于 1024，所以他还是不能给企业总部的任何服务器端口发送报文。

#### 3. 过滤 ICMP 协议

ICMP 提供了网络服务和应用程序的大量信息，如 ping 和 traceroute，管理员可以利用其协助网络管理工作，而入侵者也可以使用 ICMP 来获取局域网络上的信息，有些信息是不应该泄露出来的。但是如果没有 ICMP，网络管理程序就不能正常工作，这就是矛盾所在。由于 ICMP 信息多数是为了响应其他程序而产生的，所以过滤 ICMP 比过滤

TCP 和 UDP 都要困难。要过滤 ICMP 信息,需要从接口的进出两个方向都进行报文过滤。通常使用的 ICMP 报文有 echo request(为 ping 使用的环路测试请求)、echo reply(为 ping 使用的环路测试回应)、packet too big(某些程序用来侦测目标地址路径上的 MTU)、time to live(即 TTL,测试网络报文生存周期)、destination host unreachable(通知会话目标不可达)。如果管理员希望能 ping 和 tracerouter 分支机构的网络设备;反之不允许,则可以在路由器的配置中增加下列访问表项实现这个目的。

```
interface serial 0
ipaccess-group 100 in
ipaccess-group 101 out
access-list 100 permit icmp any 192.168.18.0 0.0.0.255 echo-reply
access-list 100 permit icmp any 192.168.18.0 0.0.0.255 packet-too-big
access-list 100 permit icmp any 192.168.18.0 0.0.0.255 ttl-exceeded
access-list 101 permit icmp 192.168.18.0 0.0.0.255 any echo-reply
access-list 101 permit icmp192.168.18.0 0.0.0.255 any packet-too-big
access-list 101 permit ip 192.168.18.0 0.0.0.255 any
```

由于访问控制列表在最末隐含 deny all,所以必须在访问控制列表 101 的最后一项加上"access-list 101 permit ip 192.168.18.0 0.0.0.255 any";否则局域网内部的计算机就无法访问分支机构的计算机了。

路由器并不能过滤所有的数据,用来允许或拒绝报文的标准是基于报文自身所包含的信息。通常,这些信息只限于报文头所包含的 OSI 参考模型的第三层网络地址和第四层的端口信息。因此,访问控制列表基本上不能使用第四层以上的信息过滤报文,比如扩展访问控制列表能够控制 ftp 报文的访问,但却不能过滤特定的 ftp 命令,如 ls 或 get 等。另外路由器对网络安全的作用是有限的,路由器并不能取代防火墙的地位,路由器主要是承担网络中的路由交换任务,同时兼顾网络安全。在中小型网络中,可以充分利用路由器的数据过滤功能,省去防火墙。但在大型的网络中,单单利用路由器是不够的。网络管理员若能充分认识路由器的功能并在工作中积极发挥路由器的安全防护作用,加强路由器的管理和配置,特别是加强访问控制列表的配置,可以有效地监控网络、过滤数据包,可以在很大程度上提高网络的安全性,为局域网络运营的正常、稳定提供有力的保障。

## 3.5 局域网安全技术策略

局域网基本上都采用以广播为技术基础的以太网,任何两个节点之间的通信数据包不仅为这两个节点的网卡所接收,同时也被处在同一以太网上的任何一个节点的网卡所截取。因此,黑客只要接入以太网上的任一节点进行侦听,就可以捕获发生在这个以太网上的所有数据包,并对其进行解包分析,从而窃取关键信息,这就是以太网所固有的安全隐患。事实上,Internet 上许多免费的黑客工具,如 SATAN、ISS、NETCAT 等,都把以太网侦听作为其最基本的手段。

### 3.5.1 网络分段方法

网络分段通常被认为是控制网络广播风暴的一种基本手段，它也是保证网络安全的一项重要措施。其指导思想在于将非法用户与网络资源相互隔离，从而达到限制和防止用户非法访问及非法侦听的目的。网络分段可分为物理分段和逻辑分段两种方式。

物理分段通常是指将网络从物理层和数据链路层（ISO/OSI 模型中的第 1 层和第 2 层）上分为若干网段，各网段相互之间无法进行直接通信。目前，许多交换机都有一定的访问控制能力，可实现对网络的物理分段。逻辑分段则是指将整个系统在网络层（ISO/OSI 模型中的第 3 层）上进行分段。例如，对于 TCP/IP 网络，可把网络分成若干 IP 子网，各子网间必须通过路由器、路由交换机、网关或防火墙等设备进行连接，利用这些中间设备（含软件、硬件）的安全机制来控制各子网间的访问。

在实际应用过程中，通常采取物理分段与逻辑分段相结合的方法来实现对网络系统的安全性控制。

通过使用网络分段，在同一个段内互相通信时只有少量的用户或设备共享同一个带宽，每个段被认为是它自己的冲突域。图 3-35 是一个分段以太网的例子，整个网络有 9 台计算机，通过把网络分成 3 个段，网络管理者减少每个段内的网络拥塞。在同一个段内传送数据时，只有 3 台计算机共享每段 10Mbps 的带宽。在一个分段的以太网局域网中，在网络主干上段与段之间的数据传送使用网桥、路由器或交换机等设备。

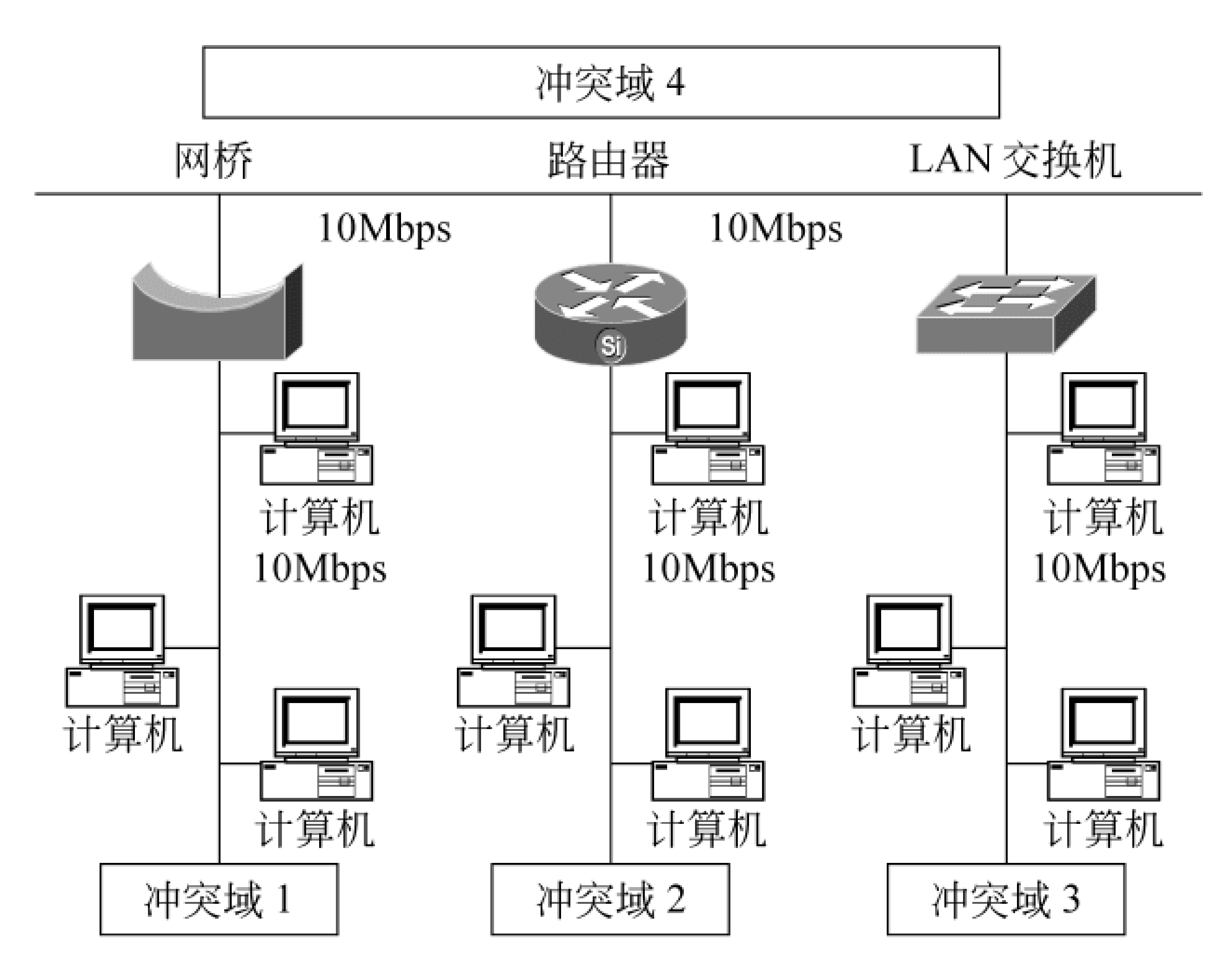



**图 3-35　物理分段的实例**

使用网络分段技术可以带来以下好处。

（1）过滤通信量。网络分段把局域网划分成不同的区域，从而减轻了局域网的负荷，同时也减小了在局域网上数据包的平均时延。

（2）扩大了物理范围。网络分段增加了局域网上工作站的总数量。从理论上讲，将局域网进行网络分段后，局域网在范围上是没有限制的（这里不仅指物理范围，还包括工作站的数量）。

(3) 提高了可靠性。当网络出现故障时,一般只影响个别网段。

(4) 减小了 Sniffer 的监听范围。网络分段后,Sniffer 只能监听它所在网段上传输的数据,而对其他网段的数据就无能为力了。

### 3.5.2 以交换式集线器代替共享式集线器方法

对局域网的中心交换机进行网络分段后,以太网被侦听的危险仍然存在。这是因为网络最终用户的接入往往是通过分支集线器而不是中心交换机,而使用最广泛的分支集线器通常是共享式集线器。这样,当用户与主机进行数据通信时,两台机器之间的数据包(称为单播包,unicast packet)还是会被同台集线器上的其他用户所侦听。一种很危险的情况是用户 Telnet 到一台主机上,由于 Telnet 程序本身缺乏加密功能,用户所输入的每个字符(包括用户名、密码等重要信息)都将被明文发送,这就给黑客提供了机会。因此,应该以交换式集线器代替共享式集线器,使单播包仅在两个节点之间传送,从而防止非法侦听。当然,交换式集线器只能控制单播包而无法控制广播包(Bmadcast Packet)和多播包(Multicast Packet)。所幸的是,广播包和多播包内的关键信息要远远少于单播包。

### 3.5.3 虚拟局域网(VLAN)的划分方法

为了克服以太网的广播问题,除了上述方法外,还可以运用 VLAN(虚拟局域网)技术,将以太网通信变为点到点通信,防止大部分基于网络侦听的入侵。VLAN 是指在局域网的物理结构上通过控制流量分配而形成的一种逻辑网络。在一个支持 VLAN 的局域网中,可以按一定的方法和规则构造多个 VLAN。一个 VLAN 中的流量被限制在本 VLAN 内,不会在其他 VLAN 中流通。这样就使 VLAN 之间逻辑上是相互隔离的,VLAN 之间的互通必须通过网桥等互联设备来实现。因此,通过 VLAN 可以在局域网中提供一定程度的数据交换安全性。通常,VLAN 是在 LAN 交换机的支持下实现的,LAN 交换机是通过标准化的 VLAN 协议(如 IEEE 802.10 或 IEEE 802.1Q)提供 VLAN 定义和管理功能的。由于利用 802.10 头中的 SAID 字段作为 VLAN 标识符,这导致了不定长的数据帧在实现上产生一些问题。另外,各个厂商所定义的 VLAN 标识符格式和长度也不统一,引起不同厂商 VLAN 设备之间兼容性问题。后来,IEEE 对 802.10 协议进行了修订,进一步完善了 VLAN 的体系结构,统一了 802.10 头中的 VLAN 标识符格式。同时,还制定了一个称为 IEEE 802.1Q 的新 VLAN 标准,并在业界得到广泛的应用。

IEEE 802.1Q 标准进一步完善了 VLAN 的体系结构,规定了统一的 VLAN 标记格式。与 VLAN 相关的协议如下。

(1) IEEE 802.1P:定义了 VLAN 中数据流优先级标记和动态组播服务,通过定义 8 个优先级支持不同的数据传输服务级别 CoS(class of service)。

(2) IEEE 802.1D:定义了第二层交换和桥接协议。这些 VLAN 协议构成了 LAN 交换机的技术基础和协议标准。

802.1P/Q 同属于一个协议集,使用同一帧格式,它们是在传统的以太网帧格式中插

入了一个标记(Tag 字段),占两个字节,如图 3-36 所示。

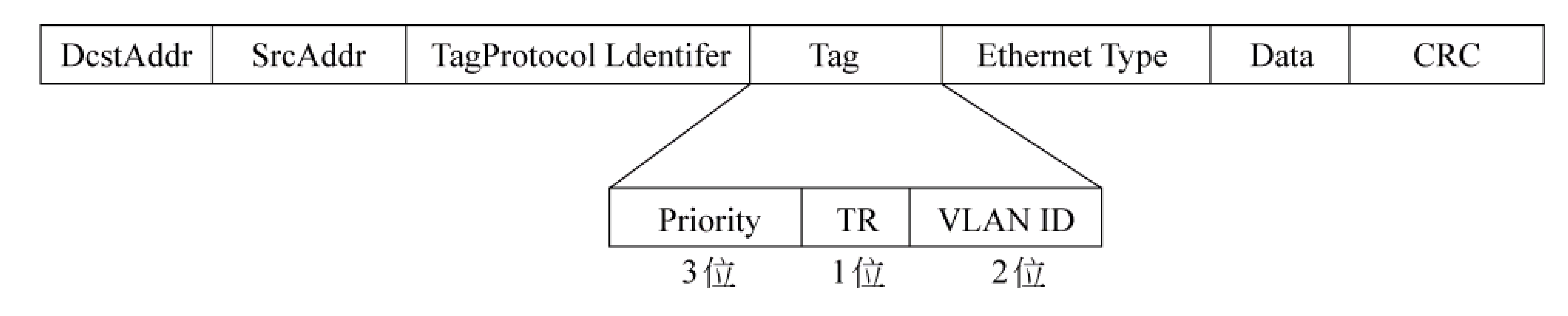



**图 3-36 IEEE 802.1P/Q 帧格式**

其中,802.1P 占 3 位,定义了 8 个优先级(prorlty);802.1Q 占 12 位,定义了 VLAN 标识符(VLAN ID),用于识别数据流所属的 VLAN。由于 VLAN 标识符共有 12 位,因此一个局域网中最多可划分 4096 个 VLAN。VLAN 除了提供局域网通信安全性外,还简化了局域网中节点的迁移操作。它既可以在保持节点物理位置不变的情况下,将节点从一个 VLAN 迁移到另一个 VLAN,也可以在保持同一 VLAN 不变的情况下,将节点移动到一个新物理位置上。所有这些迁移操作只须通过交换机所配置的 VLAN 管理软件很容易实现。因此一般高档局域网交换机都支持基于 802.10 和 802.1Q 标准的 VLAN 定义和管理功能。

目前的 VLAN 技术主要有 3 种:基于交换机端口的 VLAN、基于节点 MAC 地址的 VLAN 和基于应用协议的 VLAN。基于端口的 VLAN 虽然稍欠灵活,却比较成熟,在实际应用中效果显著,广受欢迎。基于 MAC 地址的 VLAN 为移动计算提供了可能性,但同时也潜藏着遭受 MAC 欺诈攻击的隐患。而基于协议的 VLAN,理论上非常理想,但实际应用却尚不成熟。在集中式网络环境下,通常将中心的所有主机系统集中到一个 VLAN 里,在这个 VLAN 里不允许有任何用户节点,从而较好地保护敏感的主机资源。在分布式网络环境下,可以按机构或部门的设置来划分 VLAN。各部门内部的所有服务器和用户节点都在各自的 VLAN 内,互不侵扰 VLAN 内部的连接采用交换实现,而 VLAN 与 VLAN 之间的连接则采用路由实现。目前,大多数的路由器都支持 RIP 和 OSPF 这两种国际标准的路由协议。如果有特殊需要,必须使用其他路由协议(如 Cisco 公司的 EIGRP 或支持 DECnet 的 IS-IS),也可以用外接的多以太网口路由器来代替交换机,实现 VLAN 之间的路由功能。当然,这种情况下路由转发的效率会有所下降。

无论是交换式集线器还是 VLAN 交换机都是以交换技术为核心的。它们在控制广播、防止黑客上相当有效,但同时也给一些基于广播原理的入侵监控技术和协议分析技术带来了麻烦。因此,如果局域网内存在这样的入侵监控设备或协议分析设备,就必须选用特殊的带有 SPAN(Switch Port Analyzer Network)功能的交换机。这种交换机允许系统管理员将全部或某些交换端口的数据包映射到指定的端口上,提供给连接在这一端口上的入侵监控设备或协议分析设备。下面以实例说明如何在一个典型的快速以太网局域网中实现 VLAN。所谓典型的局域网就是指由一台具备 3 层交换功能的核心交换机连接几台分支交换机(不一定具备 3 层交换能力)。假设核心交换机名称为 CEN;分支交换机分别为 DOMAIN1、DOMAIN2 和 DOMAIN3,分别通过 port1 的光模块与核心交换机相连;并且假设 VLAN 名称分别为 FINANCE、SCHEME、ADMIN。

### 1. 设置 VTP DOMAIN

VTP DOMAIN 称为管理域。交换 VTP 更新信息的所有交换机必须配置为相同的管理域。如果所有的交换机都以中继线相连,那么只要在核心交换机上设置一个管理域,网络上所有的交换机都加入该域,这样管理域里所有的交换机就能够了解彼此的 VLAN 列表。

```
CEN#vlan database                    //进入 VLAN 配置模式
CEN(vlan)#vtp domain CEN             //设置 VTP 管理域名称 CEN
CEN(vlan)vtp server                  //设置交换机为服务器模式
DOMAIN1#vlan database                //进入 VLAN 配置模式
DOMAIN1(vlan)#vtp domain CEN         //设置 VTP 管理域名称 CEN
DOMAIN1(vlan)#vtp client             //设置交换机为客户端模式
DOMAIN2#vlan database                //进入 VLAN 配置模式
DOMAIN2(vlan)#vtp domain CEN         //设置 VTP 管理域名称 CEN
DOMAIN2(vlan)#vtp client             //设置交换机为客户端模式
DOMAIN3#vlan database                //进入 VLAN 配置模式
DOMAIN3(vlan)#vtp domain CEN         //设置 VTP 管理域名称 CEN
DOMAIN3(vlan)#vtp client             //设置交换机为客户端模式
```

这里设置交换机为 server 模式是指允许在本交换机上创建修改、删除 VLAN 及其他一些对整个 VTP 域的配置参数,同步由本 VTP 域中其他交换机传递来的最新的 VLAN 信息。client 模式是指本交换机不能创建、删除、修改 VLAN 配置,也不能在 NVRAM 中存储 VLAN 配置,但可以同步由本 VTP 域中其他交换机传递来的 VLAN 信息。

### 2. 配置中继

为了保证管理域能够覆盖所有的分支交换机,必须配置中继。Cisco 交换机能够支持任何介质作为中继线,为了实现中继可使用其特有的 ISL(Inter-Switch Link)标签。ISL 是一个在交换机之间、交换机与路由器之间及交换机与服务器之间传递多个 VLAN 信息及 VLAN 数据流的协议。通过在交换机直接相连的端口配置 ISL 封装,就可以跨越交换机进行整个网络的 VLAN 分配和配置。

在核心交换机中配置如下。

```
CEN(config)#interface gigabitEthernet 2/1
CEN(config-if)#switchport
CEN(config-if)#switchport trunk encapsulation isl
CEN(config-if)#switchport mode trunk
CEN(config)#interface gigabitEthernet 2/2
CEN(config-if)#switchport
CEN(config-if)#switchport trunk encapsulation isl
CEN(config-if)#switchport mode trunk
CEN(config)#interface gigabitEthernet 2/3
CEN(config-if)#switchport
```

```
CEN(config-if)#switchport trunk encapsulation isl
CEN(config-if)#switchport mode trunk
```

在分支交换机中配置如下。

```
DOMAIN1(config)interface gigabitEthernet 0/1
DOMAIN1(config-if)#switchport mode trunk
DOMAIN2(config)interface gigabitEthernet 0/1
DOMAIN2(config-if)#switchport mode trunk
DOMAIN3(config)interface gigabitEthernet 0/1
DOMAIN3(config-if)#switchport mode trunk
```

此时,管理域设置完毕。

### 3. 创建 VLAN

一旦建立了管理域,就可以创建 VLAN 了。

```
CEN(vlan)#vlan 101 name FINANCE        //创建了一个编号为 101,名字为 FINANCE 的 VLAN
CEN(vlan)#vlan 102 name SCHEME         //创建了一个编号为 102,名字为 SCHEME 的 VLAN
CEN(vlan)#vlan 103 name ADMIN          //创建了一个编号为 103,名字为 ADMIN 的 VLAN
```

这里的 VLAN 是在核心交换机上建立的。其实只要是在管理域中的任何一台 VTP 属性为 server 的交换机上建立 VLAN,它就会通过 VTP 通告整个管理域中的所有的交换机。但是如果要将交换机的端口划入某个 VLAN,必须在该端口所属的交换机上进行设置。

### 4. 将交换机端口划入 VLAN

例如,将 DOMAIN1、DOMAIN2、DOMAIN3 分支交换机的端口 1 划入 FINANCE VLAN,端口 2 划入 SCHEME VLAN,端口 3 划入 ADMIN VLAN,则需要进行如下设置。

```
DOMAIN1(config)#interface fastEthernet 0/1        //配置端口 1
DOMAIN1(config-if)#switchport access vlan 101     //归属 FINANCE VLAN
DOMAIN1(config)#interface fastEthernet 0/2        //配置端口 1
DOMAIN1(config-if)#switchport access vlan 102     //归属 SCHEME VLAN
DOMAIN1(config)#interface fastEthernet 0/3        //配置端口 1
DOMAIN1(config-if)#switchport access vlan 103     //归属 ADMIN VLAN
DOMAIN2(config)#interface fastEthernet 0/1        //配置端口 1
DOMAIN2(config-if)#switchport access vlan 101     //归属 FINANCE VLAN
DOMAIN2(config)#interface fastEthernet 0/2        //配置端口 1
DOMAIN2(config-if)#switchport access vlan 102     //归属 SCHEME VLAN
DOMAIN2(config)#interface fastEthernet 0/3        //配置端口 1
DOMAIN2(config-if)#switchport access vlan 103     //归属 ADMIN VLAN
DOMAIN3(config)#interface fastEthernet 0/1        //配置端口 1
DOMAIN3(config-if)#switchport access vlan 101     //归属 FINANCE VLAN
DOMAIN3(config)#interface fastEthernet 0/2        //配置端口 1
```

```
DOMAIN3(config-if)#switchport access vlan 102          //归属 SCHEME VLAN
DOMAIN3(config)#interface fastEthernet 0/3             //配置端口 1
DOMAIN3(config-if)#switchport access vlan 103          //归属 ADMIN VLAN
```

## 3.6 相关安全策略考虑

在安全策略中，除了上述的方法外，对于普通用户而言，还需要注意以下几个方面的安全问题。

### 3.6.1 安全意识的培养

用户安全意识培养层面包含如下两方面含义。

**1. 网络安全管理制度的建设**

通常所说的网络安全建设“三分技术，七分管理”，也就是突出了“管理”在网络安全建设中所处的重要地位。长期以来，由于管理制度上的不完善、人员责任心差而导致的网络攻击事件层出不穷。尽管在所有的网络安全建设中，网络安全管理制度的建设都被提到极其重要的位置，但能按相关标准制定出具有全面性、可行性、合理性的安全制度并严格按其实施的项目数量并不是很多。在网络安全建设中，认真实施和执行安全制度，能从很大程度上保证网络的安全，同时为网络的管理和长期监控提供有理可依的指导性理论。例如，建立完善的机房管理制度、完善的网络使用制度、责任到人的设备管理制度、网络安全应急预案和定期网络评估制度等。

**2. 网络使用人员安全意识的培养**

通过长期分析网络安全事件，可以发现相当大的一部分攻击事件是由于工作人员的安全意识薄弱，无意中触发了入侵者设下的圈套，或打开了带有恶意攻击企图的邮件或网页造成的。针对这种情况，首要解决的问题是提高网络使用人员的安全意识，定期进行相关的网络安全知识的培训。全面提高网络使用人员的安全意识是提高网络安全性的有效手段，主要包括学习安全技术，学习对威胁和脆弱性进行评估的方法，选择安全控制的标准和实施。在无法保证安全性的情况下，了解哪些设置有危险以及密码的设置与安全等。

安全意识和相关技能的教育是企业安全管理中重要的内容，其实施力度将直接关系到企业安全策略被理解的程度和被执行的效果。为了保证安全策略的成功和有效，高级管理部门应当对企业各级管理人员、用户、技术人员进行安全培训。所有的企业人员必须了解并严格执行企业安全策略。在安全教育具体实施过程中，不同的人员有不同的安全需求。主管信息安全工作的高级负责人或各级管理人员，重点是了解、掌握企业信息安全的整体策略及目标、信息安全体系的构成、安全管理部门的建立和管理制度的制定等。负责信息安全运行管理及维护的技术人员，重点是充分理解信息安全管理策略，掌

握安全评估的基本方法,对安全操作和维护技术的合理运用等。而普通用户的重点是学习各种安全操作流程,了解和掌握与其相关的安全策略,包括自身应该承担的安全职责等。根据以上不同的需求,有针对性地对人员进行特定的安全培训。这种安全教育应当定期的、持续的进行。

尽管上面讲述了许多网络安全上的技术保证,但是事实证明,许多入侵者运用社会工程学比用黑客技术更为方便和有效。所以应该通过严格的培训使工作人员和用户不要轻易相信那些打电话给他们,要求他们做一些危及安全事情的人,如通过电话来询问密码和其他有关网络安全密码等。工作人员在透露任何有关机密前,必须明确鉴别对方的身份。另外,在实施新的系统和项目时,应该遵守目前的安全策略和设计过程,使安全人员成为项目设计阶段的一部分,并且在实施过程的早期就可以确定安全需求。在通过一项新的安全策略时,应该检查每个现有的系统与新策略是否符合,如果存在不符合的情况,则应采取措施修改它,使之符合安全策略。最好还设立内部审核部门,以便定期审核系统是否符合安全策略,并定期对每一项策略进行复查,以保证它仍然适合于机构。对于大部分策略,每年进行一次复查是合适的,如果发现与现实情况有不相适应的地方,就应当对策略进行调整,获得批准并重新开始新的用户教育过程。

### 3.6.2 用户主机保护

主机安全性主要包括客户计算机的安全防护以及到服务器的通信线路,对于提供网络服务的主机,需要通过各种技术手段进行安全防护。同样,对于普通用户的桌面系统的安全性也特别需要注意,在多数现代操作系统中,如对文件共享、个人 Web 和 FTP 服务器之类的特性使得工作站与服务器之间的安全有许多共同之处,需要遵守共同的安全准则。目前,普通用户的桌面系统主要有以下安全隐患。

#### 1. 共享过多

当用户共享本系统多于必要的范围时,就会出现由文件共享带来的较大危险。通常,如果其他用户需要看到的仅是某个目录,但却共享了整个卷(如整个驱动器)。在这里,安全危险主要来自网络内部而不是外部。用户必须认真配置防火墙,使之能阻止对文件共享连接的传送。在任何时候都不要长久地共享操作系统的主目录,如果确实需要,则应该建立特殊可共享目录而不是共享任一工作目录,可以新建一个如“D:\Share”的目录以提供访问,并确保只有此目录包含的文件才可共享。还需要保证共享在最小的范围内实施,需要认真了解如何共享文件和文件夹,不要为系统留下隐患。另外,如果用户的主机上具有重要文件或者特殊敏感信息,应当将文件加密,保证文件的安全存取。

#### 2. Web 和 FTP 服务

在常用的 Windows 操作系统中,在默认情况下并不启用 Web 和 FTP 服务器,但是可以通过其他方式对其安装并提供服务。由于 Web 和 FTP 的脆弱性,使其极容易受到攻击,带来的安全隐患主要是密码窃取。通常 FTP 服务器没有加密认证过程,所以本域用户可通过网络监听与分析捕获用户名和密码。另外,所有通过 IP 监听连接的系统容

易到拒绝服务攻击,这些攻击可以锁定用户系统的网络服务或使用户系统崩溃。如果在自己的工作用机的 Web 页中安装了任何脚本,可能会受到缓冲溢出攻击,入侵者可将恶意代码注入到用户计算机内存中,并窃取对该计算机的各种访问特权,一旦计算机受到控制,就会成为攻击其他网络的跳板。另外,不正确的配置 Web 和 FTP 服务,会提供出并不愿提供的一些共享数据。随着操作系统的不断更新,系统包含的功能越来越多,功能越来越强大,但随之而来的是潜在的危险也越来越严重。用户计算机开放的服务越多,入侵者可利用的入口就越多,所以最好关闭及删除所有用不上的服务,关闭不用的端口,以免遭受意外攻击。

### 3. 电子邮件服务

用户可能会收到来自陌生人的邮件附件,也可能会收到来自熟人意外的文件,一些宏病毒会利用 Outlook 的通讯簿将病毒复制作为附件发送给朋友,而这些朋友会毫无戒心地打开执行附件。入侵者也可能附加一个伪装的木马,如远程控制的 BO(Back Orifice)包,来控制用户计算机。通过邮件客户端传播病毒已经是一个非常普遍的现象,所以尽可能要在邮件客户端中加装了杀毒和防木马软件,用以扫描进来的信息,否则极易遭到攻击。有可能的话,使用基于 Web 方式的邮件收发,可以有效减少蠕虫病毒的扩散。

### 4. 协议安全

我们知道各种 Microsoft Windows 系统都是按在网络上运行服务的需要配置协议的,包括 NetBEUI(主要提供 Windows 联网服务,包括连接打印机,对等文件共享等)、TCP/IP、IPX/SPX(用于 Novell NetWare 文件与打印机服务以及其他相关的联网服务)等。从某种意义上来说,在网络中启用的每种协议都会有安全弱点。要确认用户所需的联网协议,禁用或删除一切不必要的协议。协议越少,意味着安全性越高。需要明确安全不是选择“正确”的协议,而是正确的使用。

### 5. 密码

对于桌面用户而言,密码保护是第一道关口。一般情况下,可以通过 BIOS 设置开机密码,然后通过操作系统设置系统密码(Windows XP 等)。建议用户为了保证系统安全,尽可能按照密码设置的要求设置密码,保证系统安全。另外,在访问一些需要密码的应用系统时,不要将密码缓存在机器中,以避免在离开时,别人可以不用输入密码就访问一些私有的信息。

### 6. 软件更新和补丁程序

实际上,没有哪个软件是安全的。软件包越大、越复杂,它的安全漏洞就越多。有些漏洞会被制造商、安全团队等发现,产品的开发商会发布更新、补丁或者围绕漏洞的工作来尽快解决该问题。一旦安全漏洞被公布,入侵者就会尝试这些新的漏洞,用户必须及时了解这些安全漏洞,并安装补丁或采取相应的措施。

### 7. 其他需要注意的

需要使用正版操作系统，并及时安装系统补丁，消除操作系统本身的安全隐患。使用正版的应用软件和工具软件，并安装防火墙及防病毒软件，还应该通过某种形式的自动更新机制来保持更新。不要安装来历不明的软件，上网时留意一些恶意插件，在没有搞清楚其具体功能时不要轻易下载安装，不要访问不良站点等，未经许可或安全咨询不要更改网络设置。

通过网络安全策略的定义与设计，有效地开发安全策略，是保证网络系统安全运行的关键。一定要牢记网络安全是一个系统，是策略、处理生命周期、技术与运行流程的结合，以及促使环境持续安全的设计方法。需要了解多种相关知识，并掌握有效的安全检测工具，如网络扫描、端口监听等工具的应用。这些工具的使用是保证网络安全有效的手段，也是系统管理员必须具备的能力。除了要求系统管理员对于整个网络系统采取各种措施外，用户本身也需要在思想上和技术上重视网络安全，安全合理地使用自己的桌面系统，加强安全管理，从而有效地保障整个网络的安全。

## 习　题　3

(1) 什么是网络安全策略？其主要内容有哪些？
(2) 考查本单位的网络，并草拟一份安全策略。
(3) 结合使用经验，谈谈如果管理好自己的计算机。
(4) 网络监听的原理是什么？常见的网络端口有哪些，并分别说明对应的应用。
(5) 从网络管理员的角度，简述局域网应采取的各种安全策略。
(6) 虚拟局域网的优势有哪些？
(7) 虚拟局域网的构建有哪几种方式？
(8) 如何制定路由器的安全策略？

# 第 4 章 chapter 4

# 操作系统安全

计算机系统由硬件系统和软件系统组成，软件系统又可以分为系统软件和应用软件。操作系统作为最基本的系统软件，它是计算机资源的直接管理者，是计算机系统的核心控制软件，也是计算机系统安全性的基础保障者。操作系统运行在硬件系统之上，为用户提供接口，用户通过接口来操作硬件系统，同时数据库、应用软件以及网络应用软件等都运行在操作系统之上。要保证这些应用软件的安全运行，除了依靠这些软件自身的安全性以外，关键还在于其底层操作系统的安全性。因此，保障操作系统的安全是保障整个计算机系统安全的基石和关键。操作系统的任何脆弱和漏洞，都会导致整个计算机系统的整体安全脆弱性。操作系统的任何功能性变化，都会导致计算机系统安全脆弱性分布情况的变化。所以，要真正解决硬件系统、数据库系统、应用软件以及网络系统的安全问题，首先要研究和开发出具有高可靠性、高容错能力和可动态配置策略的安全操作系统。

## 4.1 操作系统安全概述

### 4.1.1 操作系统安全的发展状况

操作系统安全性是计算机系统安全的基础，要妥善解决日益增多的计算机安全问题，必须要有坚固的安全操作系统作为后盾，这就要求寻找到切实有效的开发方法，从而设计出能够满足实际应用需要的安全操作系统来。早在 20 世纪 60 年代，安全操作系统的研究就引起了研究机构（尤其是美国军方）的重视，开展了大量的工作，并取得了丰富的成果。

1967 年，计算机资源共享系统的安全控制问题引起了美国国防部的高度重视，国防科学部（defense science board）旗下的计算机安全特别部队（task force on computer security）的组建拉开了操作系统安全研究的序幕。

1969 年，C. Weissman 发表了有关 Adept-50 安全控制的研究成果。安全 Adept-50 是世界上的第一个安全操作系统，可以实际投入使用。它运行于 IBM/360 硬件平台，以一个形式化的安全模型为基础，实现了美国的一个军事安全系统模型，为给定的安全问题提供了一个比较形式化的解决方案。系统支持的基本安全条件是，对于读操作不允许

信息的敏感级别高于用户的安全级别。对于写操作,在授权情况下,允许使信息从高敏感级别移向低敏感级别。

1970 年,W. H. Ware 推出的研究报告对多渠道访问资源共享的计算机系统引起的安全问题进行了研究。报告结合实际的国防信息安全等级划分体制,分析了资源共享系统中敏感信息可能受到的安全威胁,提出了解决计算机安全问题的建议途径。报告研究的主要目标是多级安全系统(multi-level security system)在计算机中的实现。

1972 年,作为承担美国空军的一项计算机安全规划研究任务的研究成果,J. P. Anderson 提出了引用监控机(reference monitor)、引用验证机制(reference validation mechanism)、安全核(security kernel)和安全建模(modeling)等重要思想。这些思想是在研究系统资源受控共享(controlled sharing)问题的背景下产生的。在受控共享和引用监控机制思想的基础上,J. P. Anderson 定义了安全核的概念。安全核是系统中与安全性的实现有关的部分,包括引用验证机制、访问控制机制、授权机制和授权的管理机制等成分。J. P. Anderson 指出,要开发安全系统,首先必须建立系统的安全模型。安全模型给出安全系统的形式化定义,正确地综合系统的各类因素。

1973 年,B. W. Lampson 通过对程序的禁闭(confinement)问题的研究提出了隐通道(covert channel)的概念。

1975 年,J. H. Saltzer 和 M. D. Schroeder 以保护机制的体系结构为中心,探讨了计算机系统的信息保护问题,重点考察了权能(capability)的实现结构和访问控制表(access control list)的实现结构,给出了信息保护机制的八条设计原则。它们是机制经济性(economy)原则、失败-保险(fail-safe)默认原则、完全仲裁原则、开放式设计原则、特权分离原则、最小特权原则、最少公共机制原则和心理可接受性原则。

1976 年,M. A. Harrison、W. L. Ruzzo 和 J. D. Ullman 提出了操作系统保护(protection)的第一个基本理论。该理论形式化地给出保护系统模型的定义,并通过三个定理给出有关保护系统的一些结果。Harrison 等还用该模型对 Unix 系统的保护系统进行了刻画。

继 Adept-50 之后,特别是 Anderson 的报告之后,越来越多的安全操作系统项目相继被启动,一系列的安全操作系统被设计和开发出来,典型的有 Multics、Mitre 安全核、UCLA 数据安全 Unix、KSOS 和 PSOS 等。原始的 Multics 操作系统虽然没有把安全性(security)列入设计目标,但保护(protection)功能的设计是一个重点。原始 Multics 中几乎所有的特权软件都在最里层保护环上。原始 Multics 的开发对安全模型和验证没有考虑,但微妙的保护结构和层次化的设计使得它成为一个比较好的增加安全性控制的基础。Mitre 安全核是基于 BLP 模型为 PDP-11 机器开发的安全核原型,性能比较差。UCLA 数据安全 Unix 是为 PDP-11 机器开发的提供 Unix 用户界面的安全核原型。KSOS(Kernelized Secure Operating System)项目的目标是为机器开发一个可投放市场的安全操作系统。PSOS(Provably Secure Operating System)是安全操作系统的一个设计项目,基于层次式开发方法,通过形式化技术实现对安全操作系统的描述和验证。

1976 年,T. A. Linden 讨论了结构化设计技术对操作系统安全性的影响,重点论述了小保护域和扩展类型的客体(extended-type object)这两个支持安全性的系统结构化思

想。小保护域可以实现程序模块级的控制,它允许一个程序中的模块运行在受到控制的环境中,防止该模块的行为对程序的其他部分造成不良的影响。

在探索如何研制安全计算机系统的同时,人们也在研究着如何建立评价标准去衡量计算机系统的安全性。第一个计算机安全评价标准的诞生,把安全操作系统研究带入了一个新的阶段。

1983 年,美国国防部颁布了历史上第一个计算机安全评价标准,这就是著名的可信计算机系统评价标准,简称 TCSEC。1985 年,美国国防部对 TCSEC 进行了修订。TCSEC 标准是在基于安全核技术的安全操作系统研究的基础上制定出来的,标准中使用的可信计算基(trusted computing base,TCB)就是安全核研究结果的表现。

1984 年,AXIOM 技术公司的 S. Kramer 发表了 LINUS IV 系统的设计与开发成果。LINUS IV 是 Unix 类的实验型安全操作系统。传统的 Unix 系统虽然提供一定的保护机制,但安全性不是它的设计目标。LINUS IV 以 4.1BSD Unix 为原型,结合 TCSEC 标准的要求,对安全性进行了改造和扩充。

1986~1987 年,IBM 公司的 V. D. Gligor 等发表了安全 Xenix 系统的设计与开发成果。安全 Xenix 是以 Xenix 为原型的实验型安全操作系统,属于 Unix 类的安全操作系统,它要实现的是 TCSEC 标准 B2-A1 级的安全要求。对 Unix 系统的原有内核进行改造和扩充,使它支持新的安全政策和 Unix 的安全政策,并保持相应的系统接口。

1988 年,AT&T Bell 实验室的 C. W. Flink Ⅱ 和 J. D. Weiss 发表了 System Ⅴ/MLS 系统的设计与开发成果。System Ⅴ/MLS 是以 AT&T 的 Unix System Ⅴ 为原型的多级安全操作系统,以 TCSEC 标准的安全等级 B 为设计目标。

1989 年,加拿大多伦多大学的 G. L. Grenier、R. Holt 和 M. Funkenhauser 发表了安全 TUNIS 系统的设计与开发成果。TUNIS(Toronto UNIversity system)是加拿大多伦多大学开发的一个与 Unix 兼容的操作系统,是 Unix 内核的一个新的实现。该系统用强类型的 Turing Plus 高级语言编写,具有较好的模块化结构。安全 TUNIS 系统内核中除安全管理器以外的其他部分构成安全机制,它能满足 TCSEC 标准的 B3 级要求。

1990 年,TRW 公司的 N. A. Waldhart 和 B. L. Di Vito 等发表了 ASOS 系统的设计与开发成果。ASOS(army secure operating system)是针对美军的战术需要而设计的军用安全操作系统,由两类系统组成,其中,一类是多级安全操作系统,设计目标是满足 TCSEC 标准的 A1 级要求;另一类是专用安全操作系统,设计目标是满足 TCSEC 标准的 C2 级要求。

1992 年,美国推出联邦标准草案,欲取代 TCSEC,消除 TCSEC 的局限性。1993 年,美国国防部在 TAFIM(technical architecture for information management)计划中推出新的安全体系结构 DGSA(DoD goal security architecture)。DGSA 的显著特点之一是对多种安全政策支持的要求,这为安全操作系统的研究提出了新的挑战,促使安全操作系统研究进入了一个新的时期。

1997 年完成的 DTOS(distributed trusted operating system)项目属于 Synergy 项目的一个组成部分。Synergy 项目是操作系统研究的一个大项目,它的目标是为安全分布式系统开发一个灵活的、基于微内核的体系结构,激励安全操作系统厂商在下一代面向

市场的操作系统中提供强大的安全机制。DTOS 每个任务包含一组线程。服务器在系统中的实现体现为一个或多个任务。端口是任务传递消息的单向通信通道。

从单一政策支持到多种政策支持,安全操作系统迈出了向实际应用环境接近的可喜一步。然而,R. Spencer 等指出,从支持多种安全策略到支持策略灵活性上来看,还有相当一段距离,支持策略灵活性的系统必须有能力对执行安全策略控制下的高级功能的低级对象进行细粒度的访问控制,必须能够确保访问权限的传播与安全政策保持一致,必须有能力撤回先前已授予的访问权限,这是处理政策变化或动态策略的需要,因为安全策略通常并不是静止的。

基于 Fluke 的 Flask 安全操作系统 Flask7 是以 Fluke 操作系统为基础开发的安全操作系统原型。Fluke 是一个基于微内核的操作系统,它提供一个基于递归虚拟机思想的、利用权能系统的基本机制实现的体系结构。Flask 是 Fluke 保障计划项目的研究成果,这个项目属于 DTOS 项目的延伸。实际上,Flask 系统的安全体系结构是从 DTOS 原型系统的安全体系结构衍生而来的。然而,虽然 DTOS 的安全体系结构是独立于特定安全政策的,但它却存在无法支持动态安全政策的不足。与此相反,Flask 的安全体系结构克服了 DTOS 体系结构中的不足,实现了动态安全政策,支持政策灵活性。

在 DTOS 项目中,美国安全计算公司(SCC)和国家安全局(NSA)开发了 DTOS 安全体系结构,该体系结构的原型建立在 Mach 微内核之上。DTOS 项目之后,Mach 微内核的工作没有得到持续的支持,因而 NSA 和 Utah 大学合作启动了 Fluke 保障计划项目,把 DTOS 安全体系结构集成到 Utah 大学开发的 Fluke 操作系统中,同时对该体系结构进行了改造,后来形成的就是 Flask 安全体系结构。

SE-Linux8 是以 Linux 操作系统为基础的基于 Flask 安全体系结构的安全操作系统。2001 年,P. Loscocco 等发布了该系统的研究成果。Flask 是基于微内核的系统原型,Linux 是非微内核的操作系统。由网络伙伴公司(NAI)的实验室、安全计算公司(SCC)和 MITRE 公司等协助 NSA 完成集成工作。NSA 已经在 Linux 内核的主要子系统中实现了 Flask 安全体系结构。在 SE-Linux8 实现中,安全服务器和 AVC 是在 Linux 操作系统中增加的两个新组件。安全服务器是 Linux 内核中的其他子系统属于客体管理器。SE-Linux8 实现的安全服务器定义了一个由类型裁决(TE)政策、基于角色的访问控制(RBAC)政策和多级安全(MLS)政策组合成的安全政策,其中 TE 和 RBAC 政策是系统实现的安全政策的有机组成,系统提供 MLS 政策支持。

相对而言,中国的安全操作系统研究起步比较晚。1993 年,国防科技大学对基于 TCSEC 标准和 UNIX System V3.2 版的安全操作系统 SUNIX 的研究与开发进行了探讨。在 SUNIX 的开发过程中,课题组的研究人员提出了一个面向最小特权原则的改进的 BLP 模型。在 SUNIX 研究工作的基础上,海军计算技术研究所按照 TCSEC 标准的 B2 安全等级的要求,围绕 UNIX System V 安全增强系统 UNIX SVR4.2/SE 的开发开展了研究工作。在"COSA 国产系统软件平台"国家"八五"科技攻关项目中,围绕着 UNIX 类国产操作系统 COSIX V2.0 的安全子系统的设计与实现工作,中国安全操作系统的研究得到了进一步的深入。中国计算机软件与技术服务总公司、海军计算技术研究所和中国科学院软件研究所等单位参加了 COSIX V2.0 安全子系统的开发工作。

COSIX V2.0 是一个基于微内核的操作系统，其安全子系统的设计目标是 TCSEC 标准的 B1＋安全等级，主要安全功能包括安全登录、自主访问控制、强制访问控制、特权管理、审计和可信通路等。1998 年，该研究所按照 TCSEC 标准的 B1 安全等级的要求对 UNIX 操作系统的内核进行了改造。

以 Linux 为代表的自由软件在中国的广泛流行对中国安全操作系统的研究与开发具有积极的推动作用。1999 年，中国科学院软件研究所推出了红旗 Linux 中文操作系统发行版本。同时，开展了基于 Linux 的安全操作系统的研究与开发工作。到 2000 年，中国的安全操作系统研究人员相继推出了一批基于 Linux 的安全操作系统开发成果，如中国科学院计算技术研究所研究开发的基于 Linux 的安全操作系统 LIDS10，南京大学开发的基于 Linux 的安全操作系统 SoftOS，中国科学院信息安全技术工程研究中心开发的基于 Linux 的安全操作系统 SecLinux。

此外，信息产业部电子第 30 研究所、国防科技大学等其他单位也以 Linux 为基础开展了安全操作系统的研究与开发工作。

### 4.1.2 操作系统安全的级别划分

评价一个操作系统是否安全以及这种安全达到了哪种程度的安全级别，需要一个评价标准来对其进行衡量。国外已经在操作系统的检测和评估方面做了大量的工作。1983 年，美国国家计算机中心发表了著名的“可信任计算机标准评价准则”(trusted computer standards evaluation criteria，TCSEC)。该标准用可信计算基(TCB)描述计算机系统中的安全支持机制，在高安全等级的要求中追求实现具备引用验证机制和安全核性质的 TCB。1985 年，美国国防部计算机安全中心(DoDCSC)对 TCSEC 文本进行了修订，推出了“DoD 可信计算机系统评估准则”。在 TCSEC 的影响下，德国、英国、加拿大等在 80 年代后期陆续推出了各自的标准，如加拿大的安全评价标准(Canadian trusted computer product evaluation criteria，CTCPEC)。CTCPEC 是专门针对政府需求而设计，该标准将安全分为功能性需求和保证性需要两部分。功能性需求共划分为四大类：机密性、完整性、可用性和可控性。每种安全需求又可以分成很多小类来表示安全性上的差别，分级条数为 0～5 级。欧洲各国的标准最终发展成统一的欧洲标准 ITSEC (information technology security evaluation criteria)。ITSEC 是欧洲多国安全评价方法的综合产物，应用领域为军队、政府和商业。该标准将安全概念分为功能与评估两部分。功能准则从 F1～F10 共分 10 级。F1～F5 级对应于 TCSEC 的 D～A，F6～F10 级分别对应数据与程序的完整性、系统的可用性、数据通信的完整性、数据通信的保密性与机密性以及完整性的网络安全。评估准则分为 6 级，分别是测试、配置控制和可控的分配、能访问详细设计和源码、详细的脆弱性分析、设计与源码明显对应以及设计与源码在形式上一致。1991 年 1 月，美国联合荷、法、德、英、加等国制定了通用信息技术安全评价标准(common criteria for IT security evaluation, CC)，并于 1996 年 1 月发布了 CC 的 1.0 版，它建立在美国的 TCSEC、欧洲的 ITSEC、加拿大的 CTCPEC 等安全评价标准的基础上，吸收了各个标准的长处和优点，从而成为一个国际通用的安全标准。

我国安全评价标准的制定工作相对较晚，于 1999 年 9 月 13 日发布。2001 年 1 月 1

日实施了中华人民共和国国家标准《计算机信息系统安全保护等级划分准则》(GB 17859—1999)(classified criteria for security protection of computer information system),其规定了计算机系统安全保护能力的五个等级,第一级为用户自主保护级,第二级为系统审计保护级,第三级为安全标记保护级,第四级为结构化保护级,第五级为访问验证保护级。实际上,我国国标是将国外的最低级 D 级和最高级 A1 级取消,余下的分为五级,TCSEC 中的 B1 级与 GB 17859 的第三级对应。GB 17859—1999 标准的制定和颁布为我国计算机信号系统安全法规的制定和执法部门的监督检查提供了依据,为安全产品的研制提供技术支持,同时也为我国安全系统的建设和管理提供了技术指导。操作系统的安全等级划分应当依据这个标准。安全操作系统应当具有我国自主版权,并且通过国家主管部门的权威测评和认证。在要求较低的场合,可以对主流操作系统进行安全加固,即在操作系统的内核之外进行安全加固,其安全功能和安全保障程度,同样必须通过国家主管部门的测评和认证。

虽然 TCSEC 可以提供很多功能,但只基本适合客户机/服务器计算时代的情况。尽管其目标令人羡慕,然而在 TCSEC 创建时,客户机/服务器计算时代才刚刚开始。到了 2004 年,C2 标准已经是一个过时的基于军事应用的标准,不能很好地在公司计算环境下工作,不能应对高等级计算机安全中的重要发展,并且难以实现网络化。另外,保证和功能相结合才能真正实现 TCSEC,而大多数环境下还不能有足够的人员支持 TCSEC 要求的安全水平。当前操作系统的设计师可以使用这些模型作为参考,选择使用能够提供最佳效果的模型,并且相应地设计出自己的系统。

国际标准化组织 ISO 开发了一个能够被作为国际应用的新的常用标准评估方法。新方法后来发展成为通用标准,其目的是综合各种国际性的和不同类型的标准成为一种新的评估信息技术产品的标准。经过努力,成为现在的国际标准 ISO 15408—1999(信息技术安全评估的国际通用标准)。它有三个区别,但又是相关的部分组成,分别有单独的文档。第一部分是对通用标准的概述,定义了信息技术评估的一般概念和原则,并介绍了评估的通用模型。第一部分还介绍了针对表现信息技术安全对象、针对选择和定义信息技术安全要求和编写产品和系统高等级技术规范的操作方法。第二部分详细介绍了具体的安全功能要求以及针对评估目标(TOC)表现安全功能要求的标准。第三部分详细介绍了安全保障要求并定义了一组保障部件作为表现 TOE 保障要求的标准方式,列出了一组保障部件、系列和类并定义了保护配置文件和安全目标的评估标准,同时还表现了针对分等级 TOE 保障定义预先定义的通用标准范围的评估保障等级,即评估保障等级(EAL)。EAL 安全评估认证等级越高,操作系统安全的可信度越高。保护配置文件(PP)和安全目标(ST)是通用标准的两个构成模块,保护配置文件定义了对具体产品类型的一组标准安全要求,这些配置文件构成了通用标准的基础。通过列出所需的产品系列安全特性的方法,通用标准允许产品说明与相关保护配置文件的相关性。在进行通用标准评估时,产品根据具体的保护配置文件进行测试,以便得出其安全能力的可靠证明。

### 4.1.3 操作系统安全的基本要求

一般而言，计算机系统的安全威胁可以归纳为软件设计和实现方面的缺陷与漏洞、系统的配置和操作不当两个主要方面。

计算机系统软件设计和实现的缺陷与漏洞包括作为计算机核心的操作系统、作为系统软件的编译器和数据库以及提供服务的应用程序等。这些软件由于功能复杂、规模庞大，如果没有安全理论的指导，因而会导致诸如缓冲区溢出、符号连接、特洛伊木马等各种各样的系统漏洞。这些漏洞一旦被发现，就会对系统的安全构成致命的威胁。TCP/IP 协议簇就是一个典型的例子，由于其在设计规划的时候没能对安全性给予足够的考虑，因此导致现在基于 TCP/IP 的各种各样的漏洞，如哄骗、会话劫持、SYN 泛洪等。

由于在使用计算机系统的过程中，对操作系统的配置和应用不当，很容易就会被攻击者突破系统的安全防范体系。一些操作系统默认的安装配置并不安全，需要根据要求对系统进行加固。经过安全配置，系统的安全性会得到较大的提高，可以抵御大部分常见的对于本系统的安全威胁。在具体应用中，这需要对应用环境有较强的理解，并需要有相当的知识储备，而一旦配置不当就会带来严重的后果。如果是系统管理员和安全管理员出现管理配置的操作失误，极有可能造成重大安全事故。

安全操作系统是在传统操作系统的基础上实现了一定安全技术的操作系统，它提供了访问控制、最小特权管理和安全审计等机制，采用各种安全策略模型，在系统硬件和资源以及用户和应用程序之间进行符合预定义安全策略的调用，限制对系统资源的非法访问和阻止黑客对系统的入侵。操作系统需要按系统安全策略对用户的操作进行存取控制，防止用户对计算机资源的非法存取；标识系统中的用户和身份鉴别；监督系统运行的安全性；保证系统自身的安全性和完整性；并能够完成特定的网络安全功能的操作。其主要功能如下。

#### 1. 进程的管理与控制

在多用户计算机系统中，必须根据不同授权范围将用户隔离，但同时又要允许用户在受控路径上进行信息交换。构造一个安全操作系统的核心问题就是具备多道程序功能，而多道程序功能得以实现又取决于进程的快速转换。

#### 2. 文件的管理与保护

包括对普通实体的管理和保护（对实体的一般性访问存取控制）和特殊实体的管理和保护（含用户身份鉴别的特定的存取控制）。

#### 3. 运行域的控制

运行域包括系统的运行模式、状态和上下文关系。运行域一般由硬件支持，也需要内存管理和多道程序支持。

### 4. 输入/输出的访问控制

操作系统安全不允许用户在指定存储区之外进行读、写操作。

### 5. 内存管理与保护

内存的管理是指要高效利用内存空间。内存的保护是指在单用户系统中，在某一时刻，内存中只运行一个用户进程，要防止它不影响操作系统的正常运行。在多用户系统中，多个用户进程并发，要隔离各个进程的内存区，防止它影响操作系统的正常运行。内存的管理与保护两者密不可分。

### 6. 审计日志管理

安全操作系统负责对涉及系统安全的操作做完整的记录以及报警或事后追查，而且还必须保证能够独立地生成、维护和保护审计过程免遭非法访问、篡改和毁坏。

## 4.1.4 操作系统安全的设计原则

操作系统安全的设计是一个复杂而艰巨的过程，涉及信息保护机制的设计和安全内核的设计。对于信息保护而言，人们以保护机制的体系结构为中心，给出了信息保护机制的八条设计原则。

### 1. 经济性原则

安全保护机制应尽可能设计得简洁，这样可以减少设计和实现错误，一旦产生这样的错误，在进行软件排错时才能较好地找到出错代码。

失败-安全默认原则：访问判定应建立在显式授权的基础上。在默认的情况下，没有明确授权的访问方式将被视做不允许的方式。如果主体想以该种方式进行访问是不会成功的，因此，对系统而言就是安全的。

### 2. 完全仲裁原则

对每一个客体的每次访问都必须经过检查，以确认是否已经得到授权。

开放式设计原则：将保护机制的抗攻击能力建立在设计公开的基础上，通过开放式的设计，在公开的环境中设法增强保护机制的防御能力。

### 3. 特权分离原则

为一项特权划分出多个决定因素，仅当所有决定因素均具备时，才能行使该项特权。

最小特权原则：分配给系统中的用户（组）或程序的特权是其能完成特定工作所必须具有的特权的最小集合。

### 4. 最少公共机制原则

把由两个以上用户共用和被所有用户依赖的机制的数量减到最小。每一个共享机

制都是一条潜在的用户间的信息通路,要谨慎设计,避免无意中破坏安全性。

#### 5. 方便使用的原则

为使安全机制能得到贯彻,系统应该为用户提供友好的用户接口,便于用户使用。在用户界面的设计上要简单易用。

对于安全内核的设计原则而言,安全内核的软件和硬件是可信的,它有三个基本的设计原则。

(1) 隔离性原则:要求安全内核有防篡改能力,即原始的操作系统要尽可能地保护自己,以防遭到偶然的破坏。在实际实施隔离原则时需要软硬件的结合。硬件的基本特性是使安全内核能防止用户程序访问安全内核代码和数据,同时还必须防止用户程序执行安全内核用于控制内存管理机制的特权指令。在拥有这些必需的硬件特性的系统中,用户程序几乎没有机会通过写入安全内核的存储器、执行特权指令或修改安全内核软件使安全内核受到直接攻击。将安全机制和操作系统的其他部分及用户空间分离,可以很容易地防止操作系统或用户的侵入。

(2) 完整性原则:要求所有信息的访问都必须经过安全内核,同时对支持安全内核系统的硬件提出要求,如果安全内核不检查每条机器指令就允许有效地执行不可信程序,硬件就必须保证程序不能绕过安全内核的存取控制。安全内核必须使各个进程独立,并且保证未通过安全内核的各个进程不能相互联系。

(3) 可验证性原则:通过利用最新的软件工程技术,注意安全内核接口功能的简单性,实现安全内核尽可能地小。支持安全内核的可验证性的基本技术是开发一个安全数学模型,其精确定义了安全需求并形式化地检验模型中的功能是否符合定义。由于内核相对很小,因此,可以进行严格的形式化证明安全内核的正确性。

### 4.1.5 操作系统的安全机制

操作系统安全的主要目标是标识用户身份及身份鉴别,按访问控制策略对系统用户的操作进行控制,防止用户和外来入侵者非法存取计算机资源,以及监督系统运行的安全性和保证系统自身的完整性等。要完成这些目标,需要建立相应的安全机制,包括硬件安全机制和软件安全机制。硬件的安全机制主要包括内存管理、运行域保护和I/O管理。软件的安全机制主要包括标识与鉴别机制、访问控制机制、最小特权管理机制、可信通路机制、隐通道的分析与处理以及安全审计机制等。

#### 1. 硬件系统的安全机制

操作系统的最底层是硬件系统,操作系统软件运行在硬件系统之上,要保证操作系统的安全运行,必然要保证硬件层操作的安全性。因此,硬件层必须提供可靠的、高效的硬件操作。硬件安全机制一般有以下三种基本的措施,分别是内存保护、运行域保护和I/O保护。

1) 内存保护

内存保护是操作系统中最基本的安全要求,它要求确保存储器中的数据能够被合法

地访问。保护单元是存储器中最小的数据范围，可以分为块、段或页等。保护单元越小，存储保护的精度越高。在多任务的环境中，应该防止用户程序访问操作系统内核的存储区域以及进程间非法访问对方的存储区域。内存保护与内存管理是紧密相关的，内存保护是为了保证系统各个进程间互不干扰以及用户进程不去非法访问系统空间，而内存管理则是为了更有效利用系统的资源(内存空间)。系统会区分用户空间和系统空间，在用户模式下运行的非特权程序应该禁止访问系统空间，而在内核模式下则可以访问任何内存空间，包括用户空间。用户模式和内核模式的切换应该通过一条特权指令来完成，这种访问控制一般可以由硬件来实现，如 Intel 的 CPU 可以运行在四个不同的等级下，其中 0 级为特权级，3 级为用户级，在 Linux 的实现中，0 级对应于内核模式，而 3 级则对应于用户模式，中间两级没有使用。除了通过硬件的限制来实现内存保护，还可以通过软件实现对内存的保护，如基于描述符的地址解释机制，该机制可以解决段/页访问权限的标识问题。在这种机制下，系统会给每一个进程分配一个私有的地址描述符，进程对系统中内存段/页的访问模式都在该描述中进行了说明，指出了该进程对内存段/页的访问模式，比如可以有两种访问模式集，一类用于在用户模式下运行的进程；另一类用于在内核模式下运行的进程。访问模式包括读、写、执行各占地址描述符的一位。因为在地址解释的同时，系统调用会检查地址描述符，所以，这种机制在运行模式切换和进程切换的过程中只需要很少的额外开销。比较适合用于内存管理的访问控制。

2）运行域保护

进程运行的区域被称为运行域。一般操作系统都会包含硬件层、内核层、应用层、用户层等几个层次，而每个层次又会包含子层。这种分层的设计方法是为了隔离运行域，达到保护运行域的目的。运行域可以看成是一系列的同心圆，最内层的特权最高，最外层的特权最低，一个进程的可信度和其访问权限可以通过它与中心的接近程度来衡量，特权等级越高则越接近中心。它是一种分级的环结构，以最底层硬件层为中心，最后到特权最低的用户层。等级域机制可以保护内层环不被其他外层环侵入。每一个进程都在特定的环层运行，特权越高的进程在环号越低的层上运行。环号越低，特权越高，相对于该层的操作保护越少。等级域机制和进程隔离机制是互不影响的，一个进程可以在任意时刻任意环内运行，在运行时还可以在各环间转移。当进程在特定环运行时，进程隔离机制将避免该进程遭受同环内其他进程的破坏，系统会隔离在同一环内同时运行的进程。此外，如果某段对于具有较低特权的环是可写的，那么在具有较高特权的环中执行它将是危险的，因为较低特权的环可能被写入了对系统具有破坏作用的代码。如果某段对于具有较高特权的环是可写的，那么在具有较低特权的环中读取该段将会导致敏感数据的泄露。因而，从安全的角度，不应该允许较低特权的环中可写的段在较高特权的环中执行，也不允许在较高特权的环中可写的段在较低特权的环中可读。

3）I/O 保护

在操作系统的所有功能中，I/O 部分一般是最复杂的。安全的缺陷往往可以从操作系统的 I/O 部分找出来，因此，为保证安全性，I/O 应该只能由操作系统才可以完成的特权操作。对于一般的 I/O 设备，操作系统都会提供该设备的系统调用。对于网络访问一般也提供标准的调用接口，用户不需要操作 I/O 的细节。I/O 设备最简单的访问控制方

式是把一个 I/O 设备看成是一个客体，所有对 I/O 设备的操作，例如读设备、写设备等，都必须经过相应的访问控制机制，如操作系统内核通过比较安全策略数据库来决定相应主体对相应客体的访问权限。在关键的安全系统中，除了采用 CPU 的隔离保护机制外，有时还需要专用的硬件如智能卡等加以进一步的保护。当然，如果要对系统提供足够的安全强度，必须将硬件和软件很好地结合起来，采用适当的安全机制才能更好保护系统。

**2. 软件系统的安全机制**

有关软件安全机制方面，主要包括身份标识与鉴别机制、访问控制机制、可信通路机制、隐蔽通道机制、安全审计和病毒防护等机制。

1）身份标识与鉴别机制

标识与鉴别是涉及系统和用户的一个过程。标识是系统要标识用户的身份，并为每个用户提供用户标识符。将用户标识符与用户联系的动作称为鉴别，为了识别用户的真实身份，它总是需要用户具有能够证明其身份的特殊信息。操作系统在开始执行操作时，首先需要用户标识自己的身份，并提供证明自己身份的依据。身份的标识与鉴别是对访问者授权的前题，并通过审计机制使系统保留追究用户行为责任的能力。一般情况下，它可以是只对主体进行鉴别，某些情况下也可以对客体进行鉴别。

2）访问控制机制

在计算机系统中，安全机制的主要内容是访问控制机制，其基本任务是防止非法用户进入系统及合法用户对系统资源的非法使用。一般来说，它包括三个任务：授权、确定存取权限和实施存取权限。在安全操作系统领域中，存取控制一般都涉及自主访问控制(discretionary access control，DAC)、强制访问控制(mandatory access control，MAC)和基于角色的访问控制(role-based access control，RBAC)几种形式。自主访问控制是一种普遍的访问控制手段，它根据用户的身份及允许访问权限决定其操作，文件的拥有者可以指定系统中的其他用户(组)对其文件的访问权。强制访问控制是指用户与文件都有一个固定的安全属性，系统用此属性来决定一个用户是否可以访问某个文件。这个属性是强制性的规定，由安全管理员或操作系统根据安全策略来确定，用户(组)或用户程序不能修改安全属性。另外，基于角色的访问控制是近年来研究的热点和重点，其基本思想是根据组织内不同职能岗位划分角色，访问许可映射在角色上，用户被分配角色来间接访问资源，用户与角色以及操作许可与角色是多对多关系，它解决了具有大量用户、数据和访问权限的系统中授权管理问题。

3）最小特权管理机制

最小特权指将超级用户的特权划分为一组细粒度的特权，分别给予不同的系统操作员/管理员，使各种系统操作员/管理员只具有完成其任务所需的特权，从而减少由于特权用户密码丢失或错误软件、恶意软件以及误操作所引起的损失。最小特权原则是系统安全中最基本的原则之一，它限定每个主体所必需的最小特权，使用户所得到的特权仅能完成当前任务。最小特权一方面给予主体"必不可少"的特权，保证了所有的主体能在所赋予的权限下完成所需要完成的操作或任务；另一方面又只给主体"必不可少"的特权，从而限制了每个主体所能进行的操作。最少特权在安全操作系统中占据了非常重要

的地位，依据最小特权原则对系统管理员的权力进行细化，每个管理员只能拥有刚好能完成工作的权限。然后根据系统管理策略设定角色，使每个角色各负其责，权限各自分立。常见的最小特权管理机制有基于文件的特权机制、基于进程的特权机制等。

4）可信通路机制

在计算机系统中，用户是通过不可信的中间应用层和操作系统相互作用的，操作系统必须保证用户在与安全核心通信时不会被特洛伊木马截获通信信息，提供一条可信通路。该机制只能由有关终端人员或可信计算机启动，并且不能被不可信软件模仿。其主要应用在用户登录或注册时，能够保证用户确实是和安全核心通信，防止不可信进程窃取密码。可信通路机制一般以安全注意键（secure attention key，SAK）为基础来实现的。当系统识别到用户在一个终端上输入的 SAK 时，便终止对应到该终端的所有用户进程，启动可信的会话过程，以保证用户名和密码不被盗走。

5）隐蔽通道机制

隐蔽通道是指系统中利用那些本来不是用于通信的系统资源绕过强制存取控制进行非法通信的一种机制。系统内充满着隐蔽通道，系统中的每一个信息，如果它能由一个进程修改而由另一个进程读取，则它就是一个潜在的隐蔽通道。隐蔽通道具有容量和带宽两个基本参数，容量是指通道一次所能传递的信息量，带宽是指信息通过通道传递的速度。由于安全模型缺陷而导致的信息泄露可以通过改变安全模型来修补，而隐蔽通道所导致的信息泄露可以在不改变安全模型的情况下消除或减少。由于隐蔽通道是允许进程以危害系统安全策略的方式传输信息的通信信道，而且出现隐蔽通道的可能性很大，因此，操作系统设计时要进行隐蔽信道详细分析测试，采取相应的措施在一定程度内清除或限制隐蔽通道。

6）安全审计机制

安全审计是指对操作系统中有关安全的活动进行记录、检查及审核，它作为一种事后追查的手段保证系统的安全性。其主要目的就是检测和阻止非法用户对计算机系统的入侵，并显示合法用户的误操作。安全审计作为安全系统的重要组成部分，在 TCSEC 中要求 C2 级以上的安全操作系统必须包含。审计为系统进行事故原因的查询、定位，事故的预测、报警以及事故发生之后的实时处理提供详细、可靠的依据和支持。一般而言，审计过程是一个独立的过程，它应与系统的其他功能隔开。操作系统必须能够生成、维护及保护审计过程，防止其被修改、访问和毁坏。特别是要保护好审计数据，严格限制未授权的用户访问。如果审计系统自身的安全被突破，审计数据的可靠性就没有保证，就不能提供准确的事后分析和追踪，也就无法估计安全事故对系统造成的影响。

7）病毒防护机制

操作系统作为一个大型的软件代码集，不可避免地会受到病毒的入侵，病毒会用它自己的程序加入操作系统或者取代部分操作系统进行工作，从而导致整个系统瘫痪。由于操作系统感染了病毒，病毒在运行时会用自己的程序片段取代操作系统的合法程序模块。根据病毒自身的特点和被替代的操作系统中合法程序模块在操作系统中运行的地位与作用，以及病毒取代操作系统的取代方式等，对操作系统进行破坏。一般来说，完全防止计算机病毒是非常困难的，但是通过安全操作系统的强制存取控制机制可以起到一

定的保护作用。当然也可以采用一些第三方的工具软件来加固操作系统的安全。

上面讲述了有关操作系统安全的一些概念与机制，下面将通过介绍目前网络中常用的两类操作系统做一些具体的说明，指导管理员对操作系统进行有效的管理，管理好操作系统是提供网络系统安全性的核心任务之一。

## 4.2 Linux操作系统的安全

Linux 是一个开放源代码的操作系统，由芬兰赫尔辛基大学的学生 Linus Torvalds 在 1991 年首先开发。世界各地的编程爱好者自发组织起来对 Linux 进行改进和编写了各种应用程序，Linux 已发展成一个功能强大的操作系统，可以自由地发行和复制。用户可以根据需要，修改其源代码，向系统添加新部件、发现缺陷和提供补丁，以及检查源代码中的安全漏洞。Linux 具有很多解决机密性、完整性、可用性以及系统安全本身问题的集成部件。包括有 IP 防御、认证机制、系统日志和审计、加密协议和 API、VPN 内核支持等。此外，系统安全可以由软件应用程序来支持，这些开放源代码的应用程序提供安全服务、加固和(或)控制 Linux 系统、防止并检测入侵、检查系统和数据的完整性，并提供防止不同攻击的屏障。

Linux 与不开放源代码的操作系统之间的区别在于开放源代码开发过程本身。由于软件的每个用户和开发者都可以访问其源代码，因而有很多人都在控制和审视源代码中可能的安全漏洞，软件缺陷很快会被发现。一方面，这会导致这些缺陷更早被利用；另一方面，很快就会有可用的安全补丁。如此反复，使得 Linux 系统在安全上表现得相当优异。也正因为这个原因，对于 Linux 操作系统的管理员而言，要求更高。如何以一种安全的方法来计划、设计、安装、配置和维护运行 Linux 的系统，是每个系统管理员需要认真考虑的问题。下面将详细论述 Linux 系统的安装配置问题、潜在的威胁以及如何保护和加固 Linux 操作系统。

### 4.2.1 Linux系统安装涉及的安全问题

Linux 系统本身是稳定和安全的，其系统安全与否和系统管理员有很大的关系。安装越多的服务，越容易导致系统的安全漏洞。在构建 Linux 操作系统时，由于默认的配置文件并不是按照安全最大化的原则来定义的。因此，在网络上利用其构建应用平台时，在安装时就必须对其各种配置文件加以了解，熟悉其配置方法、内容与特点。

在安装 Linux 系统前，首先需要系统管理员制订一个详细的安全配置计划，来确定系统将要提供什么服务，需要使用什么硬件平台，需要什么应用软件，如何组织安装。如果在实际安装前认真地制订这样一个计划，在安装的初期就可以确定并排除很多可能的安全问题。有助于减少系统入侵或者突发事件(如断电)造成系统危害的风险。而且，它为发生攻击或者发布软件漏洞和补丁时进行快速修补系统提供了一个坚实的基础。安全配置是一项比较有难度的网络技术，权限配置得太严格，好多程序又运行不起，权限配置得太松散，又很容易被黑客入侵，所以需要在系统的安全性与可用性之间找到一个平

衡。如果系统由于复杂的设置以及缺乏可用性而无法使用,那么最完善的安全特性也没有意义。此外,一些极度复杂的、极其耗费处理能力的加密算法会耗费大量系统资源,而真正需要的任务却无法正常运行使用。所以在安装系统前,需要均衡各方面因素,制订好安装配置计划。

### 1. 确定系统提供的服务和需要的软件

Linux 系统一般在网络上作为服务器对外提供各种网络服务,首先我们需要确认系统要提供哪些网络服务,以及提供这些服务的相对应的软件程序。如 Web、DNS、电子邮件、数据库等,以及包括提供这些服务所需要的相对应的软件 Apache、Bind、Sendmail、Mysql 等程序包。这些应用需求应该记录在安装部署规划之中,这个计划还包括此计算机是配置为客户机、服务器还是同时具备两个角色。由于操作系统上提供的服务越多,系统的安全漏洞就越多,系统管理员应该遵循安全原则,在安装系统时,根据需求安装一个只包含必需软件的最小化的操作系统,然后根据具体的应用需要再安装相应的软件,这样可以大大减小某个服务程序出现安全隐患的可能性,使安装好的 Linux 系统带有隐藏安全漏洞的可能性降到最低。在可能的情况下,最好每台服务器专门提供一种单一的服务,这样就会大大降低发生配置错误的可能性。

### 2. 规划用户种类和访问权限

对于网络服务器而言,规划并确定用户种类及其权限通常非常复杂。一般是根据用户的角色来分配权限,实现管理用户的权限分离,授予管理用户所需的最小权限的服务,提供严格限制默认用户的访问权限,重命名系统默认用户,修改这些用户的默认密码的服务,并禁止默认用户的访问等;对于已经确认好的用户角色,定义他们需要访问和操作(例如,读、创建、修改或删除数据)哪些数据资源。管理员可以通过访问相应的服务或操作系统提供的工具来进行相应的配置。

### 3. 选择 Linux 发行版本

由于 Linux 只是一个内核,只能提供基本的运行服务。一个完整的操作系统还包括大量的应用程序及开发工具等,因此,有许多个人、组织和企业开发了基于 GNU/Linux 的 Linux 发行版。Linux 的发行版本大体上可以分为两类,一类是商业公司维护的发行版本,一类是社区组织维护的发行版本;前者以著名的 Redhat(RHEL)为代表,后者以 Debian 为代表。选择哪一类的 Linux 系统需要管理员进行仔细的考虑。在很多情况下,由于企业的政策、企业许可证协议或者可用的技术,要使用的 Linux 发行版本已经确定。而有的时候,用户会先关注可以满足安装用途的软件程序包,然后根据程序包的先决条件、哪个发行版本包含立即可用的程序包,或者发行版本的价格,来选择发行版本。在具体的应用过程中,通常这两者是结合在一起的,用户必须反复缩小选择范围,从而选取能满足需求的发行版本。对于每一种应用服务,如邮件服务器、文件服务器、Web 服务器、字处理等,都有多种软件程序包可以满足需要。尤其当用户不直接与软件程序包打交道时(如由专门团队管理的服务器软件),那么选择更为安全的软件程序包时所受的限制就

会更少。如果要对整个发行版本进行安全评估，还需要搜索相关的安全问题邮件列表。开放源代码软件的优势之一就是能在源代码层次上对任何软件程序包进行审计，但事实上这很难做到。但是系统管理员可以做以下一些工作，将运行服务记入日志系统，从而部分实现审计功能。

(1) 启用 xinetd 来替代 inetd：这可以防止拒绝服务(denial-of-service)攻击，让管理员指定哪个服务可以提供给谁，并将服务调用日志记录到一个集中的位置。

(2) 使用 TCP 包装器：它可以将服务限制在特定范围的请求地址内，并将请求记录到日志，其配置可以通过 hosts.allow 以及 hosts.deny 文件来实现。

(3) 使用 chroot 创建安全环境：这个环境是实际安装的一个子集。它是内核中的一个系统调用，软件可以通过调用库函数，来更改某个进程所能见到的根目录，即使服务受到攻击，被影响的也只是这个子集环境。由于它基于目录树的隐藏部分，所以，它最适用于那些操作在可以方便地包括到那个树中的小的而且独立的文件集上的服务器。

#### 4. 选择服务器软件程序包

为了方便用户的安装，发行版本通常会默认安装一些保持系统运行和满足其用途所不必要的软件程序包，比如在运行没有用户交互的系统中，图形用户界面、多媒体软件和游戏都属于这种不必要的软件。而任何安装到机器上的软件都必然会占用资源并降低机器的安全性，引入可能被利用的潜在的 bug，这会导致外部攻击者利用不必要的服务在服务器上执行代码，比如通过缓存溢出破坏系统。可以减少由于安装的软件错误地配置而引起的安全漏洞。即使所安装的软件不是一直在运行，也没有暴露在网络上，它们也会增加管理员的负担。此外，有人会利用社会工程技巧来欺骗合法用户(或管理员)去运行最终影响安全的程序，这就是要尽可能少地安装程序的另一个原因。所以，系统管理员在安装 Linux 操作系统时，尽量不要使用默认安装，而应当采用选择性安装。当然，在安装系统时，为了增加系统的安全性，管理员也需要考虑额外安装一些用来增强安全性的程序包，这些程序包有的可以在用户安装系统时选择性安装，也可以安装完毕后通过手工进行补充安装。

(1) 磁盘配额：为避免本地拒绝服务攻击，管理员可以使用配额功能来限制用户(包括 httpd 或 ftpd 等后台进程的用户)可用的资源。

(2) 防火墙：防火墙通常会根据定义的规则集合管理网络通信，决定数据包是否可以通过。其基本功能是通过阻塞不必要的传输来避免网络入侵。

(3) 入侵检测：入侵检测系统的主要任务是通过识别到来的病毒、恶意软件或者特洛伊木马等安全缺口，检测进入网络或者计算机的攻击或入侵。

(4) 审计：审计是通过建立数据处于其期望状态的基线来检测敏感数据或配置文件的改变。当发生意外改变时，对基线的改变会被报告，使得管理员可以快速反应并进行恢复。

#### 5. 选用安全的工具程序版本

由于网络应用的迅速发展和成长，有些传统的应用程序在安全性上变得很脆弱，已

经不适于当前的应用。因此,人们开发了新的应用程序来替代,这些替代的程序可以以安全的方式执行相同的任务。“安全的方式”是指对传输的数据(包括用户密码和其他用户相关数据)进行加密,以防止第三方可以窃听传输的信息。使用用户名和密码或者数字签名等技术来识别用户和系统。尽管这些替代者通常被称为“安全的标准的应用程序”,但这并不是说明它们绝对不会受攻击。仅表示这些程序是用户经过深入考虑使用了,它是安全的版本而不是不安全的版本,用户不能因为使用了这些替代程序就放松安全警惕,仍需要树立安全意识和采取必要步骤来保护系统。表 4-1 列出了常见任务的应用程序及其替代产品。

**表 4-1 常见工具的安全替代**

| 任务/使用情形 | 传统应用程序 | 推荐的安全替代者 |
|---|---|---|
| 远程访问命令行 | Telnet<br>rsh(远程 SHELL) | ssh(安全 SHELL) |
| 图形方式访问远程系统 | X Window<br>VNC | 基于 ssh 的 X Window<br>基于 ssh 的 VNC<br>rdesktop |
| 文件传输 | ftp<br>rcp(远程复制) | sftp scp(安全复制) |
| 镜像/备份 | rsync | 基于 ssh 的隧道 rsync |

### 6. 规划系统硬盘分区

当选择完应用程序以及安装所使用的软件包后,下一步就是要考虑操作系统与应用程序正常运行所需要的环境,如果不考虑运行的环境或考虑太少,会引起不良后果,简单的会使系统无法正常安装,或者安装后不能正常运行,如果安装不当,还会引起系统安全性下降,特别要防止那种试图填满可用磁盘空间的 DoS 攻击带来的危害,用户需要确保至少为下面这些目录划出专门的分区:

/home:此分区包含用户数据,划出此分区的目的是使用户数据与系统无关。当执行备份和恢复操作、升级或切换操作系统,或者在系统中迁移用户时,这个独立分区就显得非常有用了。

/var:主要保存服务器的日志和运行时数据。通过将其安放于一个单独的文件系统,如果系统成为某个 DoS 攻击的目标,这样数据就不会填满系统全部的空闲空间。

/tmp:类似于/var,这个目录对用户进程来说是可写的,使得它成为 DoS 攻击的一个目标。比使用单独的文件系统更好的办法是使用 tmpfs,它加速了文件的访问速度,并在重新引导时自动清空文件系统的内容。

/boot:存放有 Linux 内核、初始驱动程序以及引导加载器数据。不必为了引导过程而挂载这个分区,因为引导加载器会将内核加载为一系列扇区,以从硬盘读取数据。如果在正常的操作中没有挂载它,那么就不会意外地覆盖这些文件。

**7. 校验软件版本**

Linux发行版本众多,人们获取的途径各有不同,可以来自于CD/DVD发行版本、从其他人那里复制、网络下载等。如果用户得到的操作系统在安装的时候就已经被破坏或已包含非法代码,那么前面所讨论的系统安全根本毫无意义,对于用户而言,这个操作系统也是毫无价值的。所以必须确保得到的操作系统是基于"干净"的来源进行安装,确认代码没有后门。一般可根据发行者公布的校验和来校验安装介质的校验和以确定介质是否为正品,通过校验MD5校验和,使用以下命令来分别判别ISO映像或者CD,来保证你得到的是一个"干净"的系统。

```
[root@test]$ md5sum /path/to/iso/image.iso
```

或

```
[root@test]$ md5sum /dev/cdrom
```

计算出的校验和必须与发行者公开的相匹配。如果通过Web得到发布的校验和,那么要确保使用https协议,并查看连接中使用的证书是否合法,以确保校验和的发布者是真实的。此外,刚刚安装的操作系统如果接入网络内提供服务,会产生大量的安全问题,因为我们得到的系统一般情况下都不是最新的版本,由于Linux系统的开放性,随时会有一些新的漏洞发现,而发行者会及时将这些安全补丁发布,而我们得到的系统可能没有安装最新安全补丁,此时最容易受到攻击。因此,在从安装过程直到完成配置步骤期间,应该从Internet上隔离出来,或者至少是在一个安全的网段。安装后,及时从相关网站上下载最新的安全补丁和更新,以便及时修补这些安全隐患。

## 4.2.2 Linux服务裁减

关闭操作系统中不必要的服务是减少漏洞、保证服务器安全最有效也是最方便的方法。在安装完操作系统后,最好进行服务裁减操作。

**1. 减少inetd的能力**

把/etc/inetd.sconf中的大部分服务都注释掉,仅仅保留所需要的部分服务。在该配置文件中没有不可以注释的部分,即所有服务都可以被注释掉。在一般情况下可以保留Telnet、FTP以及其他该服务器所提供的特殊服务,如DNS服务器的named等。

注释方法是在不使用的服务前加"#",然后reboot系统。Linux各版本内核注释方法基本相同。需要注意:Linux自身携带的FTPd在许多版本中有安全漏洞。

inetd.conf文件解释如下:

```
echo stream tcp nowait root internal
echo dgram udp wait root internal
discard stream tcp nowait root internal
discard dgram udp wait root internal
daytime stream tcp nowait root internal
```

```
daytime dgram udp wait root internal
chargen stream . tcp nowait root internal
chargen dgram udp wait root internal
```

上述这些服务都是测试的时候使用，一般均可以被注释。

```
time stream tcp nowait root internal
time dgram . udp wait root internal
```

用作时钟同步，一般可以被注释。

```
ftp stream tcp nowait root /usr/sbin/tcpd in.ftpd -l -a
```

实现文件传输协议的服务器程序，一般保留，除非服务器不提供 FTP 服务。

```
telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd
```

实现 Telnet 协议的服务器程序，一般保留，除非服务器不提供远程登录服务。

```
shell stream tcp nowait root /usr/sbin/tcpd in.rshd
```

远程 SHELL 服务，一般可以被注释(远程登录服务，上一项 Telnet 即可以实现)。

```
login stream tcp nowait root /usr/sbin/tcpd in.rlogind
```

远程注册服务，一般保留，除非服务器不提供远程登录服务。

```
exec stream tcp nowait root /usr/sbin/tcpd in.rexecd
```

远程执行服务，一般保留，除非服务器不提供远程登录服务。

```
comsat dgram udp wait root /usr/sbin/tcpd in.comsat
```

监听邮件到来，提醒用户收邮件的服务，一般可以被注释。

```
Talk dgram tcp wait root /usr/sbin/tcpd in.talkd
ntalk dgram udp wait root /usr/sbin/tcpd in.ntalkd
dtalk stream tcp wait nobody /usr/sbin/tcpd in.dtalkd
```

提供 talk 服务，一般可以被注释。

```
pop-3 stream tcp nowait root /usr/sbin/tcpd ipop3d
```

一般可以被注释，除非系统作为 E-mail 服务器，务必及时更新 POP3 的版本。

```
imap stream tcp nowait root /usr/sbin/tcpd imapd
```

实现互联网消息访问协议，一般可以被注释。

```
Uucp stream tcp nowait uucp /usr/sbin/tcpd /usr/lib/uucp/uucico - l
```

实现 UNIX 到 UNIX 的文件复制，已经被 FTP 所代替，一般可以被注释。

```
tftp dgram udp wait root /usr/sbin/tcpd in.tftpd
```

实现内部文件传输服务，一般可以被注释。

```
finger stream tcp nowait root /usr/sbin/tcpd in.fingerd
cfinger stream tcp nowait root /usr/sbin/tcpd in.cfingerd
```

提供显示本地和远程用户的服务,一般可以被注释。

```
systat stream tcp nowait guest /usr/sbin/tcpd /bin/ps - auwwx
```

向远端显示本地运行的进程,一般可以被注释。

```
netstat stream tcp nowait guest /usr/sbin/tcpd /bin/netstat - f inet
```

向远端显示本地网络状态,一般可以被注释。

```
swat stream tcp nowait.400 root /usr/sbin/swat swat
```

Samba Web 管理工具,一般可以被注释。

**2. 简单的裁减方法**

在 redhad 操作系统中可以在控制台上用超级用户(root)直接使用命令 linuxconf,进入图形化的操作界面。选择 Control(Control Panel)-Control service activity,仅保留以下服务 inet、keytable、dudzu、linuxconf(即该配置界面)、network、syslog。此外,部分 Linux 也可以在控制台上使用 setup 命令进行配置。如果可以使用 setup,则建议关闭 linuxconf 服务。

### 4.2.3 Linux用户与文件的安全管理

对于一个多用户的操作系统而言,用户(组)的管理能力对于系统整个的安全性是极其重要的。用户管理一般涉及用户的增加/删除、移走、root 用户的管理、用户密码的管理、特殊的账号管理等几个方面。

**1. 用户(组)管理**

1) 增加用户

在添加用户过程中,主要涉及以下一些关键任务。

(1) 添加用户名。

系统将用户名保存在/etc/passwd 文件中,由于此文件保存有系统上所有用户的列表,因此,需要对这个文件进行处理。管理员在进行安全配置时,在每次添加新用户后,最好复制一份文件,并将其保存在安全的地方。定期比较这两个文件的内容,一旦发现文件发生了变化,而这种变化是管理员所不知的,则本系统就有可能受到不法分子的入侵,被设置了后门。

(2) 分配用户 ID。

每个用户都被系统授予一个适当的用户 ID(UID)。UID 在系统上必须是唯一的。一般情况下,UID 使用大于 100。在设定时,由于 root 的 UID 为 0,所以,绝对不能将其他用户的 UID 设为 0。Linux 操作系统使用 UID 来识别系统中的文件所有者,所以,尽量使用系统自动分配的 UID,以避免 UID 的重复使用。

(3) 分配组 ID。

每个用户属于一个主要组,系统管理员根据用户的身份来分配组 ID,普通用户可以直接使用系统自动分配的 ID。组 ID 的信息保存在文件/etc/group 里。

(4) 定义登录后使用的 SHELL。

添加用户时,系统会为用户分配一个 SHELL,以便用户登录到系统时,能够操作计算机。常用的 SHELL 有 bash、ksh 或 csh。现在常用的是 bash,有些 Linux 版本将其设定为默认 SHELL。当然,如果用户对于某种特点的 SHELL 比较熟悉,也可以将初始 SHELL 设成自己需要的。用户在进入系统后,也可以自行进行 SHELL 的切换。不打算登录的用户或者一些应用系统的用户,只能分配一个非命令解释程序,一般根据需要设定为 nologin 或者其他的内容。

(5) 设定用户密码。

系统内置的工具都提供了指定初始密码的提示。有关密码的设定,下面会有一些具体的讲述,就不做详细论述了。

(6) 创建用户主目录。

一般而言,管理员要为每个用户分配一个主目录,主目录的路径在文件/etc/passwd 中指定。root 用户在为用户创建了目录后,要使用 chown 命令将目录的拥有者修改为用户,具体命令格式如下。

```
[root@ test]chown <username> <directory name>
```

2) 删除用户

删除用户与添加用户的工作正好相反,首先在/etc/passwd 和/etc/group 文件中删除用户的入口项,然后删除用户的 HOME 目录和所有文件。

# rm -r /usr/loginname 命令删除整个目录树,如果用户在/usr/spool/cron/crontabs 中有 crontab 文件,也应当删除。也可以利用 userdel 来删除用户或者在图形界面下处理。

3) 用户组的管理

可以使用用户组的添加命令 groupadd 和 groupdel 来增添、删除用户。所有的命令都是通过对配置文件/etc/group 的操作来完成的。/etc/group 文件含有关于组的信息,/etc/passwd 中的每个 GID 在本文件中都有相应的入口项。入口项中列出了小组名和小组中的用户,这样可方便地了解每个小组的用户,否则必须根据 GID 在/etc/passwd 文件中从头至尾地寻找同组用户。/etc/group 文件对小组的许可权限的控制并不是必要的,因为系统用 UID 来控制文件的权限,而 GID 存在于/etc/passwd 中,即使/etc/group 文件不存在于系统中,具有相同的 GID 用户也可以小组的存取许可权限共享文件。用户组就像登录用户一样可以有密码。如果/etc/group 文件入口项的第二个域为非空,则将被认为是加密密码。newgrp 命令将要求用户给出密码,然后将密码加密,再与该域的加密密码比较。需要注意的是,给组建立密码不是个好的管理习惯,这会给系统安全,特别是组用户的文件管理带来很大的隐患。

要增加一个新组,必须编辑 group 文件,为新组添加一个入口项。由于用户登录时,

系统从/etc/passwd文件中取GID,而不是从/etc/group中取GID,所以,group文件和密码文件应当具有一致性。对于一个用户的小组,UID和GID应当是相同的。多用户小组的GID应当不同于任何用户的UID。目前系统都提供了一些工具,会自动为新加的用户或组分配相应的GID和UID。但在一些特殊的情况下,还是需要修改这几个文件,管理员需要理解这些文件的用途。

**2. 用户密码的安全**

对于Linux/Unix系统来说,密码的安全至关重要。当把所有的东西都保存在计算机上,要防止别人查看这些信息的方法就是用密码把计算机保护起来。但无法破解的密码是不存在的,只要给足时间和资源,所有的密码都能破解出来。而其中通过社会工程或其他方法获得服务器的密码是最简单和最流行的入侵服务器的方法。

作为一个系统管理员,定期运行一下密码破解程序,是保证系统安全的好方法。这有利于尽早地发现和替换那些很容易被猜出来的密码,并且需要有一个好的密码检查机制,在用户选择新密码或改变旧密码的时候,排除那些有安全隐患的密码。那些字典里的单词、全是大写或全小写的以及没有包含数字或特殊字符的字符串是不能用来作密码的。建议用下面的规则选择有效的密码。

(1) 密码至少要有6个字符,最好包含一个以上的数字或特殊字符。

(2) 密码不能太简单,不要用自己的名字、电话号码、生日、职业或者其他个人信息作为密码,这种密码很容易猜出来。

(3) 密码需要设定合适的有效期,在一段时间之后就要更换密码。

(4) 如果发现有人试图猜测密码,而且已经试过很多次了。在这种情况下必须作废或者重新设定密码。

装完Linux系统之后,默认的最小密码长度为5。但是这样是不够安全的,最好密码的长度能够大于8。如果要强制用户使用8个字符以上的密码,需要编辑/etc/login.defs文件,找到PASS_MIN_LEN 5这一行,改为PASS_MIN_LEN 8。这样,当用户设定的密码小于8位的话,系统会提示设定不成功,直到将密码设成8位及以上。注意login.defs是一个重要的配置文件,其中设定了许多系统的默认参数,包括密码的最长及最短有效期、UID的最小和最大数、GID的最小和最大数等。可以通过修改这个文件中的这些参数来定制其他的安全策略。

**3. root账号的安全与管理**

root账号是Linux系统中享有特权的账号。root账号是不受任何限制和制约的。因为系统认为root知道自己在做些什么,而且会按root说的做,不问任何问题。因此,可能会因为敲错了一个命令,导致重要的系统文件被删除。使用root账号的时候,要非常小心。因为安全原因,在不是绝对必要的情况下,不要用root账号登录。特别要注意的是,不在自己的服务器上的时候,千万不要在别的计算机上用root登录自己的服务器,这是非常糟糕的一件事。在用户账号中,入侵者最喜欢具有root权限的账号,这种超级用户有权修改或删除各种系统设置,可以在系统中畅行无阻。因此,在给任何账号赋予

root 权限之前，都必须仔细考虑。

#### 4. 特殊账号的处理

Linux 系统中提供了这样可能不需要的预置账号。为了系统的安全，每次升级或安装完系统后都要检查一下账号，禁止掉其中一些不必要的预置账号。如果确定不需要这些账号，可以从系统中把它们删掉。因为系统中有越多的账号，就越容易受到攻击。具体处理过程如下。

第一步，用下面的命令删除一些不必要的用户。

```
[root@ test]#userdel adm
[root@ test]#userdel lp
[root@ test]#userdel sync
[root@ test]#userdel shutdown
[root@ test]#userdel halt
[root@ test]#userdel news
[root@ test]#userdel uucp
[root@ test]#userdel operator
[root@ test]#userdel games(如果不用 X Window 服务器，可以删除这个用户)
[root@ test]#userdel gopher
[root@ test]#userdel ftp (如果没安装匿名 ftp 服务器，可以删除这个用户)
```

第二步，输入下面的命令删除一些不必要的组。

```
[root@ test]#groupdel adm
[root@ test]#groupdel lp
[root@ test]#groupdel news
[root@ test]#groupdel uucp
[root@ test]#groupdel games (delete this group if you don't use X Window Server)
[root@ test]#groupdel dip
[root@ test]#groupdel pppusers
[root@ test]#groupdel popusers (delete this group if you don't use pop server for email)
[root@ test]#groupdel slipusers
```

第三步，给系统中的用户添加或改变密码。

```
[root@ test]#useradd admin
[root@ test]#passwd admin
```

这些命令的输出如下所示。

```
Changing password for user admin
New UNIX password: somepasswd
passwd: all authentication tokens updated successfully
```

第四步，由于“不许改变”位可以用来保护文件使其不被意外地删除或重写，也可以防止有些人创建这个文件的符号连接。删除/etc/passwd、/etc/shadow、/etc/group 或/etc/gshadow 都是黑客的攻击方法。所以，要给密码文件和组文件设置不可改变位，可

以用下面的命令完成。

```
[root@ test]#chattr i /etc/passwd
[root@ test]#chattr i /etc/shadow
[root@ test]#chattr i /etc/group
[root@ test]#chattr i /etc/gshadow
```

**注意**：如果将来要在密码或组文件中增加或删除用户，就必须先清除这些文件的不可改变位，否则就不能做任何改变。如果没有清除这些文件的不可改变位，安装那些会自动在密码文件和组文件中加入新用户的 rpm 软件包的时候，在安装过程中就会出现出错的提示。

接下来对 root 的安全加固的工作就是要防止任何人都可以用 su 命令成为 root，如果不想任何人都可以用 su 命令成为 root 或只让某些用户有权使用 su 命令，那么在/etc/pam.d/su 文件中加入下面两行。

```
auth sufficient /lib/security/pam_rootok.so debug
auth required /lib/security/pam_wheel.so group=wheel
```

加入这两行之后，/etc/pam.d/su 文件如下所示。

```
#%PAM-1.0
auth sufficient /lib/security/pam_rootok.so debug
auth required /lib/security/pam_wheel.so group=wheel
auth required /lib/security/pam_pwdb.so shadow nullok
account required /lib/security/pam_pwdb.so
password required /lib/security/pam_cracklib.so
password required /lib/security/pam_pwdb.so shadow use_authtok nullok
session required /lib/security/pam_pwdb.so
session optional /lib/security/pam_xauth.so
```

这两行的意思是只有 wheel 组的成员才能用 su 命令成为 root。注意，wheel 组是系统中用于这个目的的特殊账号，不能用别的组名。

由于在/etc/pam.d/su 配置文件中定义了 wheel 组，现在介绍一下怎样让一些用户加入到 wheel 组，从而可以用 su 命令成为 root。如果想让 admin 用户成为 wheel 组的成员，用如下的命令操作。

```
[root@ test]#usermod -G10 admin
```

其中，G 是表示用户所在的其他组，10 是 wheel 组的 ID 值，admin 是我们加到 wheel 组的用户。用同样的命令可以让其他的用户加入到 wheel 组，从而可以用 su 命令成为 root。

### 4.2.4 Linux 系统安全加固方法

在系统连接到网络之前进行加固，以避免受到攻击。下面将讨论最小化安装、授权/认证、本地和网络安全、攻击和如何防御攻击以及数据安全、病毒和恶意程序。在完成初

步计划并准备和执行了最小化安装后，需要系统管理员进行一些配置步骤。这些步骤通常被称做是加固 Linux。主要包括保护引导过程、保护服务和后台进程、保护本地文件、强制实行配额和限制及更新和添加安全补丁。

### 1. 保护引导过程

LILO 是 Linux 上一个多功能的引导程序。它可以用于多种文件系统，也可以从软盘或硬盘上引导 Linux 并装入内核，还可以作为其他操作系统的“引导管理器”。配置引导加载器，使系统在引导时不被任何用户干涉，防止用户在引导提示期间向内核传递参数。除非需要远程引导(比如在远程的数据中心)，不然就配置它要求输入密码。这是对有可能物理上接触机器的人的进一步防范。它可以防止某些事件的偶然攻击，比如使用参数 single 或者 init=/bin/sh 来获得 root shell 等。根(/)文件系统对 LILO 来说很重要，LILO 要告诉内核到那里去找根文件系统，同时 LILO 需要用到的引导扇区、/boot 目录和内核都存放在根文件系统中。引导扇区包括 LILO 引导程序的第一部分，这个部分在引导阶段的后半部分还要装入更大的引导程序。这两个引导程序通常存在/boot/boot.b 文件中。

因为 LILO 对 Linux 系统非常重要，所以需要很好地保护好它。LILO 最重要的配置文件是/etc/lilo.conf 文件。用这个文件可以配置或提高 LILO 程序以及 Linux 系统的安全性。Lilo.conf 中有三个重要的选项设置。

1) timeout=00

这项设置设定 LILO 在引导默认的系统之前，等候用户输入的时间。C2 安全等级规定这个时间间隔必须设成 0，因为多重引导会使系统的安全措施形同虚设。除非想用多重引导，否则最好把这项设成 0。

2) restricted

当 LILO 引导的时候，输入参数 linux single，可以进入单用户(single)模式。因为单用户模式没有密码验证，所以可以在 LILO 引导时，加上密码保护。restricted 选项只能和 password 合起来用。注意要给每个内核都要加上密码保护。

3) password=password

用单用户模式启动 Linux 系统的时候，系统要求用户输入这个密码，密码是大小写敏感的。而且要让/etc/lilo.conf 文件，除了 root 之外，其他用户没有读的权限，这样也就看不到密码了。下面是用 lilo.conf 文件保护 LILO 的具体步骤。

(1) 编辑 lilo.conf 文件(vi /etc/lilo.conf)，加上或改变下面介绍的设置。

```
Prompt
timeout=00                    //将这里修改成 00
default=linux
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
message=/boot/message
lba32
```

```
restricted                    //加入本行
password=password             //将 password 修改成你的密码
image=/boot/vmlinuz-2.4.20-8
        label=linux
        initrd=/boot/initrd-2.4.20-8.img
        read-only
```

(2) 因为/etc/lilo.conf 配置文件里，存在没有经过加密的密码，所以，只有 root 才能有读的权限。用下面的命令改变文件的权限。

```
[root@test]#chmod 600 /etc/lilo.conf (will be no longer world readable).
```

(3) 使改变后的/etc/lilo.conf 配置文件生效。

```
[root@test]#/sbin/lilo -v
```

(4) 为了更安全一点，可以用 chattr 命令给 lilo.conf 文件加上不可改变的权限。让文件不可改变用下面的命令。

```
[root@test]#chattr i /etc/lilo.conf
```

这样可以避免 lilo.conf 文件因为意外或其他原因而被改变。如果想要改变 lilo.conf 文件，必须先清除它的不可改变标志。清除不可改变的标记采用下面的命令。

```
[root@test]#chattr -i /etc/lilo.conf
```

### 2. 保护服务和后台进程

服务的安全配置的第一个步骤就是禁用所有不需要的服务。一些不必要的服务，不但给安全带来巨大隐患者，而且消耗系统资源，因此将不需要服务禁用，使其不会被潜在的入侵者所利用，可以有效地降低风险。同时，要禁用不安全的服务，并使用更为安全的应用程序来取代它们。例如，Telnet 不是加密的，尽量使用加密的 ssh 服务来取代 Telnet。为了找出所有启用的服务，需要检查若干个文件，如/etc/inittab 和/etc/init.d 中的引导脚本和 inetd/xinetd 中的后台进程。

1) /etc/inittab

在引导过程中，init 进程会去读取/etc/inittab 文件中的条目。完整的文件格式如下。

```
#Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
id: 3: initdefault:
```

```
#System initialization.
si:: sysinit: /etc/rc.d/rc.sysinit
l0: 0: wait: /etc/rc.d/rc 0
l1: 1: wait: /etc/rc.d/rc 1
l2: 2: wait: /etc/rc.d/rc 2
l3: 3: wait: /etc/rc.d/rc 3
l4: 4: wait: /etc/rc.d/rc 4
l5: 5: wait: /etc/rc.d/rc 5
l6: 6: wait: /etc/rc.d/rc 6
#Trap CTRL-ALT-DELETE
ca: : ctrlaltdel: /sbin/shutdown -t3 -r now
#When our UPS tells us power has failed, assume we have a few minutes
#of power left.  Schedule a shutdown for 2 minutes from now.
#This does, of course, assume you have powerd installed and your
#UPS connected and working correctly.
pf: : powerfail: /sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
#If power was restored before the shutdown kicked in, cancel it.
pr: 12345: powerokwait: /sbin/shutdown -c "Power Restored; Shutdown Cancelled"
#Run gettys in standard runlevels
1: 2345: respawn: /sbin/mingetty tty1
2: 2345: respawn: /sbin/mingetty tty2
3: 2345: respawn: /sbin/mingetty tty3
4: 2345: respawn: /sbin/mingetty tty4
5: 2345: respawn: /sbin/mingetty tty5
6: 2345: respawn: /sbin/mingetty tty6
#Run xdm in runlevel 5
x: 5: respawn: /etc/X11/prefdm -nodaemon
```

每一个条目和每一行都定义了在特定的条件下运行哪些程序。这些程序或者本身是服务,或者是用于启动和停止服务。/etc/inittab 中条目的格式是,前面是条目的标签,随后是在哪些运行级下此条目要执行,然后是动作关键字以及包括命令行参数的需要执行的命令。所有这些域都用冒号隔开。

init 进程能识别并定义运行级(run levels)的状态。当输入了运行级或者发生特定的事件(比如电源故障)时,就会考察那些条目,并执行适当的命令。

系统定义了如下 6 个运行级别。

0:关机。不要把系统的默认级别设置为 0,否则系统不能正常启动。

1:单用户模式。用于 root 用户对系统进行维护,不允许其他用户使用主机。

2:多用户模式。在该模式下不能使用 NFS。

3:完全多用户模式。主机作为服务器时,常在该模式下。

4:未分配使用。

5:图形登录的多用户模式。用户在该模式下可以进行图形界面的登录。

6:重新启动。不要把系统的默认级别设置为 6,否则不能正常启动。

如果图形登录不是必需的，为了减少不必要的应用，建议系统的默认级别设定为3。

```
id: 3: initdefault:
```

为了保护Linux系统，用户应该理解/etc/inittab中所有条目的功能，并禁用潜在不必要的服务，将其删除或者在那一行的开头使用#号注释掉它。在所有Linux系统中，都会有以下两类条目，第一类用来启动名为/sbin/getty（或者类似的）的程序，这些通常是用来允许通过Linux虚拟控制台或者串行线登录；第二类运行/etc/rc.d目录中通常名为rc的脚本，并将当前运行级作为参数给出。

2）/etc/init.d中的引导脚本

/etc/init.d中的引导脚本用来启动或者停止系统服务。每一个运行级都有一个/etc/rcN.d目录（N是运行级的标识），其中包含了指向那些在运行级改变时需要调用的脚本的链接。如果链接文件名以S开头，则脚本在进入那个运行级时被执行，启动相应的服务；如果以K开头，则脚本在退出那个运行级时被执行，停止那个服务。大部分情况下，引导脚本的名称会指示它所控制的服务，如rc3.d目录下的S55sshd表明在进入运行级3时，会启用sshd服务。要防止在特定的运行级中会启动某个服务，则删除运行级目录中指向相应引导脚本的链接，或者使用一个不做任何事情的虚脚本取代/etc/init.d中原来的引导脚本即可。

3）inetd/xinetd中的后台进程

可以在客户机请求时根据需要调用服务。这些请求被转交给超级后台进程inetd或者xinetd。然后超级后台进程确定要启动哪个服务，并将请求传递到相应的后台进程。通常，Telnet、ftp、rlogin等服务使用inetd或者xinetd启动。

（1）inetd的管理。

inetd也叫做“超级服务器”，inetd.conf是inetd的配置文件，位于/etc目录下，它指挥inetd监听哪些网络端口，为相应的端口启动相应的服务。不需要的服务应该被禁止掉，最好将其卸载，这样系统的漏洞就少一些。禁止任何不需要的服务，具体过程如下。

① 将inetd.conf文件的许可权限改成600，保证除了root用户外，其他用户不能读写并执行。

```
[root@ test]#chmod 600 /etc/inetd.conf
```

② 编辑inetd.conf文件（vi /etc/inetd.conf），禁止所有不需要的服务，如ftp、telnet、shell、login、exec、talk、ntalk、imap、pop-2、pop-3、finger、auth等。修改后的文件具体格式如下。

```
#ftp stream tcp nowait root /usr/sbin/tcpd in.ftpd -l - a
#telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd
#
#Shell, login, exec, comsat and talk are BSD protocols.
```

③ 改变了inetd.conf文件之后，重启inetd进程，使修改生效。给inetd进程发一个SIGHUP信号（killall -HUP inetd）。

```
[root@deep /root]#killall -HUP inetd
```

④ 用 chattr 命令把它设成不可改变，来保证 inetd. conf 文件的安全，把文件设成不可改变位要用下面的命令。

```
[root@test]#chattr i /etc/inetd.conf
```

这样可以避免 inetd. conf 文件的任何改变(意外或是别的原因)。一个有 i 属性的文件是不能被改动的，不能删除也不能重命名，不能创建这个文件的连接，不能往这个文件里写数据。只有系统管理员才能设置和清除这个属性。如果要改变 inetd. conf 文件，必须通过以下命令先清除这个不允许改变的标志。

```
[root@test]#chattr -i /etc/inetd.conf
```

(2) 从安全角度出发，新的 LINUX 分发包大多采用 xinetd 代替了 inetd。与 inetd 相比，xinetd 能够启动基于 rpc 的服务，并支持访问控制，可以限制进入连接的速度、来自特定主机的连接数目，或者某个服务的总连接数。xinetd. conf 是 xinetd 的配置文件，它位于/etc 目录下。

```
#Simple configuration file for xinetd
#Some defaults, and include /etc/xinetd.d/
defaults
{
        instances               = 60
        log_type                = SYSLOG authpriv
        log_on_success          = HOST PID
        log_on_failure          = HOST
        cps                     = 25 30
}
includedir /etc/xinetd.d
```

文件最后一行表示 /etc/xinetd. d 目录是存放各项网络服务(包括 http、ftp 等)的核心目录，因而系统管理员需要对其中的配置文件进行熟悉和了解。一般说来，在/etc/xinetd. d 的各个网络服务配置文件中，每一项都有下列形式。

```
service service-name
{
      Disabled                //表明是否禁用该服务
      Flags                   //可重用标志
      Socket_type             //TCP/IP 数据流的类型，包括 stream、datagram、raw 等
      Wait                    //是否阻塞服务，即单线程或多线程
      User                    //服务进程的 uid
      Server                  //服务器守护进程的完整路径
      log_on_failure          //登录错误日志记录
}
```

其中，service 是必需的关键字，且属性表必须用大括号括起来。每一项都定义了由

service-name 定义的服务。service-name 是任意的，但通常是标准网络服务名，也可增加其他非标准的服务，只要它们能通过网络请求激活，包括 localhost 自身发出的网络请求。每一个 service 有很多可以使用的 attribute(属性)，操作符可以是"＝"、"＋＝"或"－＝"。所有属性可以使用"＝"，其作用是分配一个或多个值。某些属性可以使用"＋＝"或"－＝"的形式，其作用分别是将其值增加到某个现存的值表中，或将其值从现存值表中删除。

每一项用户想新添加的网络服务描述既可以追加到现有的/etc/xinetd. conf 中，也可以在/etc/xinetd. conf 中指定的目录中分别建立单独的文件。建议采用后一种做法，因为这样可扩充性很好，管理起来也比较方便，用户只需要添加相应服务的描述信息即可追加新的网络服务。在该目录中使用如下命令可以看到许多系统提供的服务。

如果想要开启 Telnet 服务，只需要通过使用 vi 编辑器改写该文件为如下内容。然后，使用/etc/rc. d/init. d/xinetd restart 命令来激活 Telnet 服务即可。

```
service telnet
{
    disable= no                    //将该域置为 no,则表明开启该服务
    lags= REUSE
    socket_type= stream
    wait= no
    user= root
    server= /usr/sbin/in.telnetd
    log_on_failure+ = USERID
}
```

如果想要关闭某个不需要的服务，则将上述的"disable ＝ no"改为"disable ＝ yes"即可。为了更详细地访问控制，xinetd 支持以下三个另外的参数：only_from、no_access 和 access_time。

以 Telnet 服务为例，说明其用法。为了限制访问，但不完全禁用 Telnet 后台进程，可以对配置文件/etc/xinetd. d/telnet 进行如下修改。

```
service telnet
{
   disable= no
   flags= REUSE
   socket_type= stream
   wait= no
   user= root
   server= /usr/sbin/in.telnetd
   log_on_failure+ = USERID
      only_from          = 192.168.200.3 192.168.200.7 192.168.200.9
      only_from         + = 192.168.200.10 192.168.200.12 172.16.0.0
      no_access          = 172.16.{1,2,3,10}
      access_times       = 07:00-21:00
```

}

only_from 和 no_access 可以接受数字 IP 地址(最右边的零作为任意数值处理)、IP 地址/网络掩码范围、主机名以及/etc/networks 中的网络名。如果组合使用 only_from 和 no_access,xinetd 会为每个主机连接寻找最接近的匹配。在前面的代码示例中,表示 IP 地址为 172.16.x.x 的主机可以连接到此主机,但地址属于 172.16.1.x、172.16.2.x、172.16.3.x 和 172.16.10.x 的则不能连接。可见,当使用 no_access 所用的因数符号时,不需要指定地址的所有四个部分,因数部分必须是地址最右边的部分。

每次修改了配置文件后,为使修改生效,需使用/etc/rc.d/init.d/xinetd restart 命令来启用最新的配置。

### 3. 进程保护

Linux 在运行时,会产生大量的进程,如何找出并禁用那些不必要的或者具有潜在危险的进程,需要管理员弄清楚哪些进程正在用户的系统中实际地运行,并禁用那些不需要的进程。同时需要定期地检查不正常的行为,定期审计。查看是否有未知的进程在运行,因为这些未知的进程可能会提供不必要的服务,可能会带来系统的损害。

理想情况下,用户应该明白在自己的系统中运行的每一个进程。要获得所有进程的列表,可以执行命令 ps -ef。显示的进程列表中有方括号的是内核级的进程,执行辅助功能(比如将缓存写入到磁盘);其他所有进程都是使用者进程。用户会注意到,就算是在用户新安装的(最小化的)系统中,也会有很多进程在运行。要熟悉它们,并把它们记录到文档中。

```
[root@ test]#ps -ef
UID         PID  PPID  C STIME TTY          TIME CMD
root          1     0  0 Feb06 ?        00:00:04 init [3]
root          4     1  0 Feb06 ?        00:00:00 [ksoftirqd_CPU0]
root          9     1  0 Feb06 ?        00:00:00 [bdflush]
root          5     1  0 Feb06 ?        00:00:17 [kswapd]
root          6     1  0 Feb06 ?        00:00:00 [kscand/DMA]
root          7     1  0 Feb06 ?        00:00:00 [kscand/Normal]
root          8     1  0 Feb06 ?        00:00:00 [kscand/HighMem]
root         10     1  0 Feb06 ?        00:00:00 [kupdated]
root         11     1  0 Feb06 ?        00:00:00 [mdrecoveryd]
root         15     1  0 Feb06 ?        00:00:24 [kjournald]
root         73     1  0 Feb06 ?        00:00:00 [khubd]
root       2796     1  0 Feb06 ?        00:00:00 [kjournald]
root       3088     1  0 Feb06 ?        00:00:06 syslogd -m 0
root       3092     1  0 Feb06 ?        00:00:00 klogd -x
root       3142     1  0 Feb06 ?        00:00:04 /usr/sbin/sshd
root       3153     1  0 Feb06?   00:00:00 xinetd -stayalive -reuse -pidfile /var
/run/xinetd.pid
root       3163     1  0 Feb06 ?        00:00:01 crond
```

```
root        3170       1   0 Feb06 tty2        00:00:00 /sbin/mingetty tty2
root       19879       1   0 Feb09 tty1        00:00:00 /sbin/mingetty tty1
root       30175    3142   0 06:38 ?           00:00:00 /usr/sbin/sshd
root       30177   30175   0 06:38 pts/0       00:00:00 -bash
root       30256   30177   0 06:43 pts/0       00:00:00 ps -ef
```

开放网络连接的进程受到攻击的潜在可能最大。要获得所有 TCP 或 UDP 连接的列表,可以执行命令 netstat -atu(附带名字解析,易读)或者 netstat -atun (没有名字解析,更快)。在这个列表中,特别要注意状态为 LISTEN 的 TCP 连接和所有的 UDP 连接,因为服务器通过这些连接来接收到来的连接请求。

确定这些进程是如何被启动的(通过/etc/inittab、通过引导脚本等)并禁用它们。如果程序是由另一个程序启动的,那么这项任务需要管理员非常熟悉系统,如 X 服务器很有可能是由显示管理器(xdm、kdm 或 gdm)启动的,其本身并不会出现在 inittab 或引导脚本目录中。

netstat 所列出的连接并不是都可以由网络上的所有计算机来使用。在任何数据包到达开放的连接之前,基于 Linux 内置功能的防火墙可以进一步控制访问。

### 4. 保护文件系统

保护文件系统涉及文件和目录的所有者及访问它们的权限。要保护文件系统,文件和目录的保护位必须设置为只授予最小限度的权限。要特别注意关于所有人可写的文件和系统目录的不适当权限,以及所谓的 setuid 或者 setgid 命令。这些命令运行时的用户权限比运行此命令的用户实际拥有的权限更高,这对于访问只有 root 才有权限访问的文件来说这可能是必需的。举个例子来说,/etc/shadow 文件由于存有用户的加密密码信息,对系统的安全至关重要,因此权限很严,只有 root 才有权限其可读可写。但是系统必须允许普通用户也能修改自己的密码。要想让他们对/etc/shadow 可写,又不能可读,而且可写又不能允许他们改别人的密码,如何处理这种情况呢? 系统做一个程序,即 bin 目录下的 passwd,通过它可以在不显示文件内容的情况下直接修改 /etc/shadow 文件,这个程序由系统赋予它 setuid 权限,而且它属于 root。这样用户在使用 /bin/passwd 改密码时就有 root 权限。由于/bin/passwd 命令本身功能的局限性,用户并不能用它做更多的不利于系统安全的事。对于这种命令,要确保它们每一个都确实需要设置 setuid/setgid 位。如果程序或文件没有这种需要的话,需要禁用它。要找出所有人都可写的文件,使用以下命令。

```
[root@ test]#find / -perm -002 \( -type f -o -type d \) -ls
```

其中:

/是搜索的起始位置。

-perm 检查权限。

002 表示(八进制符号)other 设置了写位。

模式 002 之前的 - 表示设置了所有权限位(没有考虑模式中的 zero-bits)。

-type f 或者-type d 搜索常规的文件和目录。

-ls 以 ls 格式列出找到的文件。

找到文件后，要对列出的文件进行分析判断，并进行相应的处理。

当某个分区上的所有文件确实都不需要 setuid/setgid 位时，可以利用/etc/fstab 中的 nosuid 选项为相应文件系统中的每个文件都禁用它，如示例中的 /dev/hdc1)。

```
#device        mountpoint    filesystemtype    options       dump    fsckorder
/dev/hda1    /         ext2         defaults     1    1
...
/dev/hdc1    /mnt/cdrom    iso9660        nosuid,user     1    2
```

此外，对于所有敏感的数据，都有必要对其进行加密并使用密码保护它。

1）异常和隐含文件

在系统的每个地方都要查看一下有没有异常和隐含文件，因为这些文件可能是隐藏的黑客工具或者其他一些信息（密码破解程序、其他系统的密码文件等）。在 Linux/UNIX 操作系统下，一个常用的技术就是用一些特殊的名，如"..."、".. "（点点空格）或"..^G"（点点 control-G），来隐含文件或目录。用"find"程序可以查找到这些隐含文件。

```
[root@ test]#find / -name ".. " -print - xdev
[root@ test]#find / -name ".* " -print -xdev | cat -v
```

2）查找任何人都有写权限的文件和目录

如果入侵者获得并改变了一些系统文件，这些系统文件就会成为安全漏洞。任何人都有写权限的目录也同样有危险，因为入侵者可以根据他们的需要自由地添加或删除文件。在正常情况下有些文件是可写的，包括一些/dev 目录下的文件和符号连接。在系统中定位任何人都有写权限的文件和目录用下面的命令。

```
[root@ test]#find / -type f ( -perm -2 -o -perm -20 ) -exec ls -lg {}
[root@ test]#find / -type d ( -perm -2 -o -perm -20 ) -exec ls -ldg {}
```

3）查找没有主人的文件

发现没有主人的文件就意味着有黑客入侵系统了。不能允许没有主人的文件存在。如果在系统中发现了没有主人的文件或目录，先查看它的完整性，如果一切正常，给它一个主人。有时候卸载程序可能会出现一些没有主人的文件或目录，在这种情况下可以把这些文件和目录删除掉。定位系统中没有主人的文件用下面的命令。

```
[root@ test]#find / -nouser -o -nogroup
```

**注意**：不用管/dev 目录下的那些文件。

4）查找.rhosts 文件

查找.rhosts 文件是日常管理工作的一部分，因为这些文件不允许在系统中存在。记住，黑客有可能只要有一个账号就可能入侵整个网络。可以用下面的命令定位系统中的.rhosts 文件。

```
[root@ test]#find /home -name .rhosts
```

也可以用一个 cron 任务定期地查看、报告和删除 $HOME/.rhosts 文件。同时，也

必须让用户知道系统会经常地进行这种审核。

### 5. 强制实行配额和限制

Linux PAM(插入式认证模块,Pluggable Authentication Modules)可以强制实行一些实用的安全限制,可在/etc/security/limits.conf文件中对此进行配置,这些限制适用于单个对话。用户可以使用maxlogins来控制总额限制。limits.conf中的条目有如下结构:username|@groupname type resource limit。

为了与username区别,groupname之前必须加@。类型必须是soft或者hard。软限制(soft-limit)可以被超出,通常只是警戒线,而硬限制(hard-limit)不能被超出。resource可以是下面的关键字之一。

core 限制内核文件的大小(KB)。

data 最大数据大小(KB)。

fsize 最大文件大小(KB)。

memlock 最大锁定内存地址空间(KB)。

nofile 打开文件的最大数目。

rss 最大持久设置大小(KB)。

stack 最大栈大小(KB)。

cpu 以分钟为单位的最多CPU时间。

nproc 进程的最大数目。

as 地址空间限制。

maxlogins 此用户允许登录的最大数目。

在下面的代码示例中,所有用户每个会话都限制在10MB,并允许同时有四个登录。第三行禁用了每个人的内核转储。第四行除去了用户bin的所有限制。ftp允许有10个并发会话(对匿名ftp账号尤其实用)。managers组成员的进程数目限制为40个。developers有64MB的memlock限制,wwwusers的成员不能创建大于50MB的文件。

```
*             hard   rss         10000
*             hard   maxlogins       4
*             hard   core            0
bin           -
ftp           hard   maxlogins      10
@managers     hard   nproc          40
@developers   hard   memlock     64000
@wwwusers     hard   fsize       50000
```

要激活这些限制,用户需要在/etc/pam.d/login文件底部添加下面一行"session required/lib/security/pam_limits.so"。配额让用户能够限制用户和组的inode数目和可用空间。

**注意:**配额是在每个加载点上定义的,如果用户在若干个分区上有写权限,那么要确保为它们每个都定义配额。

配额是管理员最小化 DoS 攻击的一种方式，这类攻击以填满硬盘驱动器上所有可用空间为手段，这会使其他进程因不能创建临时文件而失败。必须在内核中启用配额。当前大部分发行版本都支持配额。要为文件系统启用配额，需要在/etc/fstab 中为相应的行添加一个选项。使用 usrquota 和 grpquota 来启用用户配额和组配额，如下所示。

```
/dev/hda1     /             ext3     defaults                       1 1
/dev/hda2     /home         ext3     defaults,usrquota              1 1
/dev/hda3     /tmp          ext3     defaults,usrquota,grpquota     1 1
/dev/hda4     /shared       ext3     defaults,grpquota              1 1
/dev/hdc1     /mnt/cdrom    iso9660 nosuid,user                     1 2
```

然后，使用 mount -a -o remount 重新挂载相应的文件系统，来激活刚才添加的选项。再使用 quotacheck -cugvm 创建一个二进制配额文件，其中包含了机器可读格式的配额配置，这是配额子系统要操作的文件。

使用工具 edquota 完成配额的指派，如要为用户 alice 定义限制，则使用 edquota -u alice 来调用它。环境变量 editor 中定义的编辑器 vi 会打开，其中有类似如下的内容。

```
Quotas for user alice:
/dev/hda2:  blocks in use:  3567, limits (soft=5500, hard=6500)
            inodes in use:  412, limits (soft=1000, hard=1500)
```

in use 值只是为用户提供信息，不能被修改，管理员能修改的只是软限制和硬限制。保存并退出编辑器后，edquota 会读取用户刚才编辑的临时文件，并将那些值传递到二进制配额文件，以使用户的修改生效。对组配额的编辑与此相同，只是必须使用-g 选项而不是-u。软限制是警告级别，可以被超出，而硬限制是严格强制的。软限制有一个宽限期(grace period)，有时也称为软性时间限制(soft time limits)，这是允许用户超出软限制直到被系统强制执行之前的时间间隔。使用 edquota -t 来设置宽限期，可以使用的单位是秒、分、小时、天、周和月。其他管理配额的实用工具包括 repquota(总结某个文件系统的配额)、quotaon 和 quotaoff(打开和关闭配额)。

### 4.2.5 Linux 系统安全管理

通过用上面的方法对 Linux 服务器进行安装和一些基本的设置后，服务器的安全性得到了相当的提高。接着要进行服务器的管理，成功管理系统的关键之一是要知道系统中正在发生什么事，而日志是了解 Linux 系统运行情况的唯一方法。系统再安全，总还是会有入侵者可以通过各种方法利用系统管理员的疏忽侵入系统。但其一举一动都会记录到系统的日志之中，尽管他们可能可以改变这些日志信息，甚至用自己的程序替换掉系统本身的命令程序，但是通过日志把所有的连接都记录下来，可以发现攻击者试图进行的攻击。下面主要讲一下 Linux 环境中的系统日志管理和系统审计以及怎么用一些工具更加方便有效地管理日志信息。

#### 1. 日志文件

Linux 日志存储在 /var/log 目录中。这里有几个由系统维护的日志文件，但其他服

务和程序也可能会把它们的日志放在这里。大多数日志只有 root 才可以读，这些日志文件为系统的安全状态提供了信息。这里主要讲解两个日志守护程序 syslog 和 klogd，并且简要叙述由 Linux 操作系统生成的其他日志文件。

（1）syslog：大部分的 Linux 系统中都要使用 syslog 工具，它使系统根据不同的日志输入项采取不同的活动。syslog 工具由一个守护程序组成，能接受访问系统的日志信息并且根据/etc/syslog.conf 配置文件中的指令处理这些信息。任何希望生成日志信息的程序都可以向 syslog 接口呼叫生成该信息。通常 syslog 接受来自系统的各种功能的信息，每个信息都包括重要级。syslogd 根据设备和信息重要级别来报告信息。syslog 守护程序是由/etc/rc.d/init.d/syslog 脚本在运行级 2 下被调用的，默认不使用选项。但有两个选项-r 和-h 很有用。如果要使用一个日志服务器，必须调用 syslogd -r。默认情况下 syslog 不接受来自远程系统的信息。当指定-r 选项后，syslogd 将会监听从 514 端口上进来的 UDP 包。如果还希望日志服务器能传送日志信息，可以使用 -h 标志。默认时，syslogd 将忽略使其从一个远程系统传送日志信息到另一个系统的/etc/syslog.conf 输入项。

（2）klogd：klogd 守护进程获得并记录 Linux 内核信息。通常，syslogd 会记录 klogd 传来的所有信息。然而，如果调用带有-f filename 变量的 klogd 时，klogd 就在 filename 中记录所有信息，而不是传给 syslogd。当指定另外一个文件进行日志记录时，klogd 就向该文件中写入所有级别或优先权。klogd 中没有和/etc/syslog.conf 类似的配置文件。使用 klogd 而不使用 syslogd 的原因在于可以查找大量错误。如果有人入侵了内核，使用 klogd 可以修改错误。

在/var/log 和不同版本的系统中以及自己配置的应用程序中都可以找到其他日志文件。当然，/etc/syslog.conf 列出了由 syslogd 管理的所有日志文件名和位置。其他日志由其他应用程序管理，如 cron 工具维护的信息日志文件/var/log/cron，当系统重新配置时将生成日志文件。

保证在/var/log 目录下的不同日志文件的完整性是保证系统安全所要考虑的非常重要的一个方面。所以，有必要创建重要的日志文件的硬复制。如果在服务器上已经加上了很多安全措施，黑客还是能够成功入侵，那么日志文件就是最后的防范措施，保证日志文件的完整性就显得非常重要。如果服务器上或网络中的其他服务器上已经安装了打印机，就可以把重要的日志文件打印出来。这要求有一个可以连续打印的打印机，并用 syslog 把所有重要的日志文件传到/dev/lp0（打印设备）上。入侵者可以改变服务器上的文件、程序等，但把重要的日志文件打印出来之后，他就无能为力了。例如，需要记录下服务器上所有的 telnet、mail、引导信息和 ssh 连接，并打印到连接在这台服务器上的打印机上。只要在/etc/syslog.conf 文件中加入以下一行。

```
authpriv.* ;mail.* ;local7.* ;auth.* ;daemon.info /dev/lp0
```

重新启动 syslog daemon 使改动生效。

```
[root@ test]#/etc/rc.d/init.d/syslog restart
```

还可以将要记录的服务器上所有的 telnet、mail、引导信息和 ssh 连接的日志文件复

制到别的服务器上。把所有日志文件复制到其他计算机上，从而可以在一台计算机上管理多台计算机的日志文件，从而简化管理工作。具体步骤是先编辑接收日志文件的服务器（如 logserver. test. com）上的 syslog. conf 文件（vi /etc/syslog. conf），在文件的末尾加入下面这一行：

```
authpriv.* ;mail.* ;local7.* ;auth.* ;daemon.info /dev/lp0
```

因为 syslog daemon 的默认配置是拒绝接收来自网络上的信息，必须使它能够接收来自网络上的信息，在 logserver 接收日志文件服务器上的脚本文件 syslog daemon 中加入下面的-r 参数。编辑 syslog 脚本文件（vi /etc/rc. d/init. d/syslog），把 daemon syslogd -m 0 改为“daemon syslogd -r -m 0”。

重新启动 syslog daemon 使改动生效。

```
[root@ test]#/etc/rc.d/init.d/syslog restart
```

最后，编辑一下发送日志文件的服务器上的 syslog. conf 文件（vi /etc/syslog. conf），在末尾加上这一行：

```
authpriv.* ;mail.* ;local7.* ;auth.* ;daemon.info @ logserver
```

logserver 是接收日志文件的计算机主机名。如果有人试图入侵服务器并且威胁把所有重要的系统日志文件都删掉，这样就不用怕了，因为已经将日志打印出来或者在别的地方还有一个复制。管理员就可以根据这些日志文件分析出入侵者在什么地方，然后处理这次入侵事件。有关 syslogd 程序的其他一些参数和策略，可以用 man 命令查看帮助：syslogd(8)、syslog(2)和 syslog. conf(5)。

**2. 系统审计**

Linux 系统审计主要有连接审计和进程审计。连接审计是跟踪当前用户当前对话、用户登录和退出的活动。在 Linux 系统中使用 utmp（动态用户对话）和 wtmp（登录/退出日志记录）工具来完成这一审计过程。wtmp 工具还同时维护重新引导和系统状态变化信息。各种程序对这些工具进行刷新和维护，因此无须进行特殊的后台进程或程序。然而 utmp 和 wtmp 输出结果文件必须存在，如果这些文件不存在会关闭连接审计。与 utmp 和 wtmp 有关的所有数据将分别保存在/var/run/utmp 和/var/log/wtmp 中，这些文件归 root 用户所有。

last 和 who 是出于安全角度定期使用的最常用命令。last 命令提供每一个用户的登录时间、退出登录时间、登录位置、重新引导系统及运行级别变化的信息。last -10 表示 last 的最多输出结果为最近的 10 条信息。默认时，last 将列出在/var/log/wtmp 中记录的每一连接和运行级别的变化。从安全角度考虑，last 命令提供了迅速查看特定系统连接活动的一种方式。观察每天的输出结果是个好习惯，从中可以捕获异常输入项。last 命令的-x 选项可以通知系统运行级别的变化。who 命令主要作用是报告目前正在登录的用户、登录设备、远程登录主机名或使用的 X Windows 的 X 显示值、会话闲置时间以及会话是否接受 write 或 talk 信息。其他的有关命令有 lastlog 命令，该命令报告了有关

/var/log/lastlog 中记录的最后一次登录的数据信息。

Linux 的进程审计是对进程活动的记录。一般由 psacct 程序来完成，有的 Linux 分发包已安装，有的没有安装，需要根据所采用的系统安装使用 psacct。它提供了几个进程活动监视工具：ac、lastcomm、accton 和 sa。

ac 命令显示用户连接时间的统计。

lastcomm 命令显示系统执行的命令。

accton 命令用于打开或关闭进程记账功能。

sa 命令统计系统进程记账的情况。

原始数据保存在 /var/log/pacct 文件中，其许可权限为 600。该文件的存在是进程审计有效的保障。与连接审计不同，进程审计必须处于打开状态，使用下面的命令设置打开状态。

```
[root@ test]#accton  /var/log/pacct
```

可以使用自选文件代替 /var/log/pacct，但必须记住这一文件并且设置适当的许可权限。必须在每次引导的时候执行该命令，可以在/etc/rc.d/rc.local 中输入以下脚本。

```
#  initiate  process account
if  [-x  /sbin/accton  ]
then
/sbin/accton   /var/log/pacct
echo  "process  accounting  initiated"
fi
```

一旦在系统中配置进程审计后，就可以利用这些工具来监视用户的命令和时间。

ac 命令可以根据登录数/退出数在屏幕上打印出用户的连线时间(单位为小时)。总计时间也可以打印出来。如果执行没有任何参数的 ac 命令，屏幕将会显示总计的连线时间。

sa 是一个统计命令。该命令可以获得每个用户或每个命令的进程使用的大致情况，并且提供了系统资源的消费信息。在很大程度上，sa 又是一个审计命令，对于识别特殊用户，特别是已知特殊用户使用的可疑命令十分有用。另外，由于信息量很大，需要处理脚本或程序筛选这些信息。可以用这样的命令单独限制用户。

```
[root@ test]#sa -u |grep test
```

输出结果从左到右依次为用户名、CPU 使用时间秒数、命令(最多为 16 个字符)。

lastcomm 命令提供每一个命令的输出结果，同时打印出与执行每个命令有关的时间印戳。就这一点而言，lastcomm 比 sa 更有安全性。lastcomm 命令使用命令名，用户名或终端名作为变量。该命令可以查询进程审计数据库。

```
[root@ test]#lastcomm test
```

下面显示 lastcomm test 的输出结果，每行表示命令的执行情况，从左到右为用户、设备、使用的 cpu 时间秒数、执行命令的日期和时间。

```
reboot      test   ttyp1   0.01   secs  Fri  Feb 26  18:40
tcpdump     test   ttyp1   0.01   secs  Fri  Feb 26  18:39
lastcomm    test   ttyp1   0.01   secs  Fri  Feb 26  18:32
ls          test   ttyp1   0.01   secs  Fri  Feb 26  18:30
```

如果系统被入侵,就不要太相信在 lastlog、utmp、wtmp、pacct 中记录的信息,因为这些信息可能被修改过了。通常在已经识别某些可疑活动后,进程审计可以有效地发挥作用。使用 lastcomm 可以隔绝用户活动或在特定时间执行命令。但是使用该命令必须设置为打开状态。基本上,/var/log/pacct、/var/run/utmp、/var/log/pacct 是动态数据库文件。其中/var/log/pacct 和/var/log/wtmp 文件随着输入项的增加和修改而增加。解决文件过于庞大的方法,可以通过 logrotate 程序来解决上面这个问题,该程序通过读取/etc/logrotate. conf 配置文件,该配置文件告诉 logrotate 所要读/etc/logrotate. d 目录中的文件,ls 可以通过它来设定日志文件的循环时间。

### 3. 更新和添加安全补丁

由于 Linux 固有的特点,发行版本更新较快,系统只有尽快保持更新,才可能在安全上得到有效保障,所以,管理员需要及时了解系统软件和应用软件的修订和补丁。通常软件提供商和 Linux 发行商会在网站上为用户及时地提供这些信息。用户也可以使用 CERT(computer emergency response team)提供的安全服务。当有新的更新可用时,管理员应该去查看它是否适用于本系统以及系统的安全需要。安装更新本身可能会导致安全问题。还要考虑到每个更新都可能会引入新的漏洞,或者如果更新失败,用户的系统可能会停留在不可用的状态。当在大范围的系统中安装某个更新时,可能会导致用户的多个系统在更新期间互相不兼容。所以,更新系统会涉及很多风险。要降低风险,需要注意以下几点。

(1) 初始安装后,不要将用户的系统立即连接到网络。将所有相关的更新下载到一台单独的机器,然后手工地传输它们,以确保系统暴露在网络上之前已经处于当前状态。

(2) 管理员需要对系统进行更新前进行备份,始终拥有可用的近期系统备份。在出现问题后能及时恢复系统。

(3) 对于业务中每一个关键的系统,建议建设一个与产品环境的硬件和软件相同的独立测试环境。先在测试环境中更新,如果成功,再应用到真实的应用系统,以防止在管理产品系统时出现意外。保证在修改产品环境之前,测试环境中的主要功能和服务不会受到影响。

(4) 制订安装更新的计划,要考虑更新系统的次序、对用户的业务来说关键的系统、系统如何互相依赖以及哪个系统包含机密数据等问题。

(5) 在安装任何修订之前,要使用密码检验和工具检查软件的完全性和真实性(尤其是通过网络下载的软件)。

### 4. 系统备份

完成 Linux 系统的安装以后,需要对整个系统进行备份,主要是为了以后可以根据

这个备份来验证系统的完整性,发现系统文件是否被非法篡改过。而且当发生系统崩溃时,也可以通过备份来恢复到正常的状态。无论采用怎样的安全措施都不能完全消除系统崩溃的可能性,系统的安全性和可靠性是与备份密切相关的。定期备份对安全而言是非常重要的,可使系统在灾难发生后将其恢复到一个稳定的状态,并将损失降到最小程度。备份的常用类型有三种:零时间备份、整体备份和增量备份。系统的备份应根据具体情况制定合理的策略,备份文档应经过处理(压缩、加密等)合理保存。

Linux/Unix 系统中有几个专门的备份程序,分别是 dump、restore 和 backup。网络备份程序有 rdump/rstore、rcp 和 rdist 等。最安全的备份方法是把它们备份到别的地方,如磁带、可写光盘、网络存储等,可以参考相关资料学习使用方法。

## 4.2.6 其他的一些安全技术

Linux 的安全涉及的面比较广,除了上述一些安全注意事项外,还包括一些需要了解的安全知识,主要涉及以下几个方面。

### 1. 部分文件及应用的安全措施

1) 禁止使用控制台程序

禁止使用所有的控制台程序,这是最简单而且最常用的保证系统安全的方法。可以运行下面的命令来实现。

```
[root@ test]#rm -f /etc/security/console.apps/servicename
```

这里 servicename 是要禁止的控制台程序名。除非使用 xdm,否则不要把 xserver 文件删掉,否则除了 root 之外,没有人可以启动 X 服务器了。如果使用 xdm 启动 X 服务器,这时 root 是唯一需要启动 X 服务器的用户,这才有必要把 xserver 文件删掉。

```
[root@ test]#rm -f /etc/security/console.apps/halt
[root@ test]#rm -f /etc/security/console.apps/poweroff
[root@ test]#rm -f /etc/security/console.apps/reboot
[root@ test]#rm -f /etc/security/console.apps/shutdown
[root@ test]#rm -f /etc/security/console.apps/xserver
```

这些命令可以禁止所有的控制台程序:halt、poweroff、reboot 和 shutdown。只有装了 X Window,删除 xserver 文件才会有效果。

**注意**:根据前一章介绍安装的服务器,X Window 是没有安装上的,上面说的那些文件可能不会出现在/etc/security 目录下,如果这样就可以不管这一节介绍的方法。为了禁止所有的控制台访问,包括程序和文件,需要将/etc/pam.d/目录下的所有文件中包含 pam_console.so 的行加上注释。

2) TCP_WRAPPERS

在默认情况下,Linux 允许所有的服务请求。可以用 TCP_WRAPPERS 来保护服务器的安全,使其免受外部的攻击。需要在/etc/hosts.deny 文件中加入"ALL: ALL@ALL,PARANOID"以禁止所有计算机访问服务器,然后在/etc/hosts.allow 文件中一个

一个加入允许访问服务器的计算机。这种做法是最安全的。

TCP_WRAPPERS 是由两个文件控制的，依次是/etc/hosts. allow 和/etc/hosts. deny。判断是依次进行的，如果在/etc/hosts. allow 文件中有匹配的项(daemon、client)，那么允许访问。否则，查看/etc/hosts. deny，如果找到匹配的项，那么访问被禁止，否则访问被允许。

(1) 编辑 hosts. deny 文件(vi /etc/hosts. deny)加入下面这些行。

```
Access is denied by default.
#Deny access to everyone.
ALL: ALL@ALL, PARANOID #Matches any host whose name does not match its address, see bellow.
```

这样做的意思是所有的服务、访问位置如果没有被明确地允许，也就是在/etc/hosts. allow 中找不到匹配的项，就是被禁止的。

**注意：** 加上 PARANOID 参数之后，如果要在服务器上使用 telnet 或 ftp 服务，就要在服务器的/etc/hosts 文件中加入允许使用 telnet 和 ftp 服务的客户端计算机的名字和 IP 地址。否则，在显示登录提示之前，因为 DNS 的域名解析，可能要等上几分钟时间。

(2) 编辑 hosts. allow 文件(vi /etc/hosts. allow)。如被授权访问的计算机的 IP 地址是 192. 168. 186. 1，主机名是 gate. test. com，允许使用的服务是 sshd。那么需要做如下配置。

```
sshd:   192.168.186.1 gate.test.com
```

(3) 用 tcpdchk 检查 TCP_WAPPERS 配置的程序。它检查 TCP_WAPPERS 的配置，并报告它可以发现的问题或潜在的问题。在所有的配置都完成了之后，运行 tcpdchk 程序即可。

```
[root@ test]#tcpdchk
```

3) 修改/etc/aliases 文件

aliases 文件如果管理错误或管理不善也会造成安全隐患。例如，很多的软件厂商都把 decode 这个别名放在 aliases 文件里。这样做是为了方便通过 E-mail 传送二进制文件。在发送邮件的时候，用户把二进制文件用 uuencode 转成 ASCII 文件，然后把结果发给接收端的 decode。由这个别名让邮件信息通过/usr/bin/uuencode 程序把二进制文件重新转换成 ASCII 文件。如果允许 decode 出现在 aliases 文件中，可以想象将会有什么样的安全隐患。所以，把定义 decode 这个别名的行从 aliases 文件中删除。同样地，每一个会运行程序的别名都要好好查看一下，很有可能要把它们删除掉。编辑 aliases 文件(vi /etc/aliases)，删除或注释掉下面这些行。

```
#Basic system aliases -- these MUST be present.
MAILER-DAEMON:   postmaster
postmaster:   root
#General redirections for pseudo accounts.
bin:   root
daemon:   root
```

```
#games:  root          //remove or comment out
#ingres:  root         //remove or comment out
nobody:  root
#system:  root         //remove or comment out.
#toor:  root           //remove or comment out
#uucp:  root           //remove or comment out
#Well-known aliases.
#manager:  root        //remove or comment out
#dumper:  root         //remove or comment out.
#operator:  root       //remove or comment out
#trap decode to catch security attacks
#decode:  root
#Person who should get root's mail
#root:  marc
```

修改完毕,要使改动生效,还必须运行以下程序。

```
[root@ test]#/usr/bin/newaliases
```

4) 使系统对 ICMP 包没有响应

TCP/IP 协议本身有很多的弱点,黑客可以利用一些技术,把传输正常数据包的通道用来偷偷地传送数据。防止系统对 ping 请求做出响应,对于网络安全很有好处,因为没人能够 ping 你的服务器并得到任何反应,使系统把这个危险减到最小。用下面的命令阻止 ICMP 包。

```
[root@ test] echo 1> /proc/sys/net/ipv4/icmp_echo_ignore_all
```

运行完这个命令后,系统对 ping 就没有反应了。也可以直接修改 icmp_echo_ignore_all,将其值设为 1。对 ICMP 数据包没有反应,至少可以把绝大多数的入侵者排除到系统之外,因为入侵者不知道服务器在哪里。重新恢复对 ping 的响应,可以用下面的命令。

```
[root@ test] echo 0> /proc/sys/net/ipv4/icmp_echo_ignore_all
```

5) 禁止 IP 原路径路由

IP 原路径路由(IP source routing),就是 IP 数据包包含有目的地址的详细路径信息,因为根据 RFC 1122 规定,目的主机必须按原路径返回这样的 IP 包。如果入侵者能够伪造原路径路由的信息包,那么它就能截取返回的信息包,并且欺骗用户的计算机,让它觉得正在和它交换信息的是可以信任的主机,这是非常危险的,所以需要禁止 IP 原路径路由以避免这个安全漏洞。不过,在新的 Linux 分发包中,已经将这个漏洞修补,默认情况下系统禁止 IP 原路径路由,检查一下服务器目录/proc/sys/net/ipv4/conf 下的目录及文件,如果发现 accept_source_route 文件里的值为 0 的话,说明系统已将其禁止,否则请将其修改为 0。

6) 使 TCP SYN Cookie 保护生效

“SYN Attack”是一种拒绝服务(DoS)的攻击方式,它会消耗掉系统中几乎所有资

源，迫使服务器无法正常提供服务。它是采用巨大的信息流来消耗系统的资源，以至于服务器不能够响应正常的连接请求。在网络安全中，这也是常见的入侵手段。在许多Linux 内核中，syn cookie 是一个可选项，并没有使其生效。想要使其生效必须用下面的命令。

```
[root@ test]#echo 1> /proc/sys/net/ipv4/tcp_syncookies
```

用户可以将这个命令加入/etc/rc. d/rc. local 文件中，等下次系统启动的时候就不必重新输入了。

7）资源限制

限制用户对系统资源的使用，可以避免拒绝服务（如创建很多进程、消耗系统的内存等）这种攻击方式。这些限制必须在用户登录之前设定，如可以用下面的方法对系统中用户加以限制。

第一步，编辑 limits. conf 文件（vi /etc/security/limits. conf），加入或改变下面这些行。

```
* hard core 0
* hard rss 5000
* hard nproc 20
```

这些行的意思是 core 0 表示禁止创建 core 文件；nproc 20 把最多进程数限制到 20；rss 5000 表示除了 root 之外，其他用户都最多只能用 5M 内存。上面这些都只对登录到系统中的用户有效。通过上面这些限制，就能更好地控制系统中用户对进程、core 文件和内存的使用情况。星号“*”表示的是所有登录到系统中的用户。

第二步，编辑/etc/pam. d/login 文件，在文件末尾加入下面这一行。

```
session required /lib/security/pam_limits.so
```

加入这一行后“/etc/pam. d/login”文件是这样的：

```
#%PAM-1.0
auth required /lib/security/pam_securetty.so
auth required /lib/security/pam_pwdb.so shadow nullok
auth required /lib/security/pam_nologin.so
account required /lib/security/pam_pwdb.so
password required /lib/security/pam_cracklib.so
password required /lib/security/pam_pwdb.so nullok use_authtok md5 shadow
session required /lib/security/pam_pwdb.so
session required /lib/security/pam_limits.so
#session optional /lib/security/pam_console.so
```

8）控制 mount 上的文件系统

可以用一些选项，如 noexec、nodev 和 nosuid 来更好地控制 mount 上的文件系统，如/home 和/tmp。这些都可以在/etc/fstab 文件中设定。fstab 文件包含了各个文件系统的描述信息。可以编辑 fstab 文件（vi /etc/fstab），并根据需要把下面两行：

```
/dev/sda11 /tmp ext2 defaults 1 2
/dev/sda6 /home ext2 defaults 1 2
```

改变成：

```
/dev/sda11 /tmp ext2 nosuid, nodev, noexec 1 2
/dev/sda6 /home ext2 nosuid, nodev 1 2
```

nodev 表示不允许在这个文件系统上有字符或特殊的块设备。nosuid 表示不允许设定文件的 suid(set-user-identifier)和 sgid(set-group-identifier)许可位。noexec 表示不允许文件系统上有任何可执行的二进制文件。

**注意**：上面的例子中，/dev/sda11 mount 到 /tmp 目录上，而/dev/sd6 mount 到 /home 目录上。这和实际情况会有所不同，主要取决于用户是怎么分区以及用什么样的硬盘，例如，IDE 硬盘是 hda、hdb 等，而 SCSI 硬盘是 sda、sdb 等。

9）保护 rpm 程序

如果在服务器上用 rpm 命令安装完所有需要的软件，最好把 rpm 程序转移到一个安全的地方，如软盘或其他安全的地方。这样如果入侵者侵入了服务器，他也不能用 rpm 命令安装那些有害的软件。如果将来还要用 rpm 安装新的软件，只要把 rpm 程序拷回原来的目录就可以了。用下面的命令来处理 rpm 程序。

```
[root@ test]#mount /dev/fd0 /mnt/floppy/
[root@ test]#mv /bin/rpm /mnt/floppy/
[root@ test]#umount /mnt/floppy
```

**注意**：千万不要把 rpm 程序从系统中卸载掉，否则就不能重新安装它。因为安装 rpm 程序或其他软件包本身就要用 rpm 命令。还有一点要注意的是，把 rpm 命令的访问许可从默认的 755 改成 700，这样非 root 用户就不能使用 rpm 命令了。特别是考虑到万一在安装完新软件之后忘了把 rpm 程序移到一个安全的地方，这样做就更有必要了。改变/bin/rpm 程序的默认访问权限，用下面这个命令：

```
[root@ test]#chmod 700 /bin/rpm
```

10）保护登录 SHELL

为了方便重复输入很长的命令，bash SHELL 可以在～/. bash_history 文件中默认存 500 个曾经输入过的命令。每一个有自己账号的用户，在自己的目录中，都会有. bash_history 文件。可能会有这种情况，用户在不该输入密码的地方输入了密码，而输入的密码会在. bash_history 文件中保存下来，而且. bash_history 文件越大这种可能性也越大。在/etc/profile 文件中 HISTFILESIZE 和 HISTSIZE 这两行决定了系统中所有用户的. bash_history 文件可以保存多少命令。建议把/etc/profile 文件中的 HISTFILESIZE 和 HISTSIZE 都设成一个比较小的值，编辑 profile 文件(vi /etc/profile)，把这些行改成：

```
HISTFILESIZE=20
HISTSIZE=20
```

这样每个用户目录下的. bash_history 就最多只能存 20 个命令。如果入侵者试图在

用户的～/.bash_history 文件中发现一些密码，就没有什么机会了。

11）使 Control-Alt-Delete 关机键无效

把/etc/inittab 文件中的一行注释掉可以禁止用 Control-Alt-Delete 关闭计算机。如果服务器不是放在一个安全的地方，这点非常重要。编辑 inittab 文件（vi /etc/inittab）把这一行：

```
ca:: ctrlaltdel: /sbin/shutdown -t3 -r now
```

改为：

```
#ca:: ctrlaltdel: /sbin/shutdown -t3 -r now
```

用下面的命令使改变生效。

```
[root@ test]#/sbin/init q
```

12）减少登录信息

默认情况下，当登录装有 Linux 系统的计算机时，系统会告诉用户 Linux 发行版的名字、版本号、内核版本和服务器名称。这样就泄露了太多的系统信息，最好只显示一个 Login：的提示信息。

（1）编辑/ect/rc.d/rc.local 文件，在下面这些行的前面加上“#”。

```
#This will overwrite /etc/issue at every boot. So, make any changes you
#want to make to /etc/issue here or you will lose them when you reboot.
#echo "" > /etc/issue
#echo "$R" >> /etc/issue
#echo "Kernel $ (uname -r) on $a $ (uname -m)" >> /etc/issue
#
#cp -f /etc/issue /etc/issue.net
#echo>> /etc/issue
```

（2）删除/etc 目录下的 issue.net 和 issue 文件。

```
[root@ test]#rm -f /etc/issue
[root@ test]#rm -f /etc/issue.net
```

**注意**：/etc/issue.net 文件是用户从网络登录计算机时（如 Telnet、SSH），看到的登录提示。同样在/etc 目录下还有一个 issue 文件，是用户从本地登录时看到的提示。这两个文件都是文本文件，可以根据需要改变。但是，如果想删掉这两个文件，必须向上面介绍的那样把/etc/rc.d/rc.local 脚本中的那些行注释掉，否则每次启动的时候，系统又会重新创建这两个文件。

13）一些有用的系统查看命令（如表 4-2 所示）

表 4-2 系统查看命令

| 命令 | 功 能 |
|---|---|
| du | 报告在层次目录结构(当前工作目录或指定目录起)中各目录占用的磁盘块数,可用于检查用户对文件系统的使用情况 |
| df | 报告整个文件系统当前空间的使用情况,可用于合理调整磁盘空间的使用和管理 |
| ps | 检查当前系统中正在运行的所有进程,对于用了大量 CPU 时间的进程、同时运行了许多进程的用户、运行了很长时间但用了很少 CPU 时间的用户进程应当深入检查。还可以查出运行了无限制循环的后台进程的用户或未注销户头就关终端的用户(一般发生在直接连线的终端) |
| who | 可以告诉系统管理员系统中工作的进展情况等许多信息,检查用户的登录时间和登录终端 |
| su | 当用户试图使用 su 命令进入系统用户时,命令将在/usr/adm/sulog 文件中写一条信息,若该文件记录了大量试图用 su 进入 root 的无效操作信息,则表明了可能有人企图破译 root 密码 |
| login | 程序记录了无效的登录企图。如果无效登录的次数突然增加,表明可能有人企图通过猜测登录名和密码 |

## 2. 查找可疑迹象

上面讨论了一些需要在系统中检查并且可能表明薄弱点或攻击,如隐藏文件、SUID 和 SGID 文件以及所有人都可以写的文件的迹象。还有其他几条途径可以检查 Linux 系统上的可疑活动。

1) 查看网卡状态

嗅探器将网卡置为混杂模式,这样就可以捕获所有经过网卡的信息。如果接口在这种模式下运行 ifconfig – a 集合,网卡会报告处于 PROMISC 状态。这是一个嗅探器正在运行的迹象。如果不是由系统管理员运行的,说明系统有遭到入侵的可能,需要对其出现的原因进行仔细调查。要关闭混杂模式,需要使用如下命令:

```
#ifconfig etho promisc down
```

2) 采用 netstat 命令检查系统

程序 netstat 用于显示在 Linux/Unix 系统上哪些网络连接被监听,采用命令 netstat – na,参数 n 告诉 netstat 不要解析主机地址。

```
[root@ wg root]#netstat -na
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp        0      0 0.0.0.0: 3306          0.0.0.0: *             LISTEN
tcp        0      0 0.0.0.0: 9005          0.0.0.0: *             LISTEN
tcp        0      0 210.29.192.22: 80      0.0.0.0: *             LISTEN
tcp        0      0 0.0.0.0: 22            0.0.0.0: *             LISTEN
tcp        0     48 210.29.192.22: 22      192.168.18.32: 2442    ESTABLISHED
udp        0      0 0.0.0.0: 514           0.0.0.0: *
udp        0      0 0.0.0.0: 805           0.0.0.0: *
udp        0      0 0.0.0.0: 69            0.0.0.0: *
Active UNIX domain sockets (servers and established)
```

```
Proto RefCnt Flags       Type       State         I-Node Path
unix   2      [ ACC ]    STREAM     LISTENING     1065342
/tmp/ssh-XXvCQFm7/agent.11519
unix   2      [ ACC ]    STREAM     LISTENING     3248    /tmp/mysql.sock
unix   2      [ ACC ]    STREAM     LISTENING     3154    /dev/gpmctl
unix   2      [ ACC ]    STREAM     LISTENING     3287    /dev/log
unix   2      [ ]         STREAM     CONNECTED     661315
unix   2      [ ]         STREAM     CONNECTED     661312
unix   2      [ ]         STREAM     CONNECTED     4917
unix   2      [ ]         STREAM     CONNECTED     4887
unix   2      [ ]         STREAM     CONNECTED     4114
unix   2      [ ]         STREAM     CONNECTED     4042
```

在本地地址栏中显示的地址以本地端口号结束,可以使用这个端口号识别连接是向内还是向外的。如果本地端口号是 23,则是一个到 telnet 后台程序的向内连接。如果本地端口号是 1035,并且外部端口号是 23,则是一个向外的 telnet 连接。

从输出中可以看到,所有带 LISTEN 的行都意味着有一个程序正在监听端口。只有管理员配置的端口才应该被监听,如果发现一个端口没有被管理员所配置,则应该对系统进行详细检查,以了解端口被打开的原因。

3) 采用 lsof 检查系统进程状况

netstat 的一个问题是它不能告诉你哪一个进程打开端口。找出哪个进程链接到了特定端口将是一项费力的工作。lsof 解决了这个问题,要查看进程状况,采用命令 lsof,具体如下。

```
[root@ wg root]#lsof -i
COMMAND     PID    USER    FD   TYPE   DEVICE SIZE NODE NAME
sshd        3161   root    3u   IPv4   3086       TCP ＊ : ssh (LISTEN)
xinetd      3173   root    6u   IPv4   3108       UDP ＊ : 805
mysqld      3243   root    3u   IPv4   3247       TCP ＊ : mysql (LISTEN)
serverSoc   3255   root    3u   IPv4   3260       TCP ＊ : 9005 (LISTEN)
syslog-ng   3270   root    3u   IPv4   3286       UDP ＊ : syslog
httpd       3280   root    3u   IPv4   3326       TCP 192.168.111.22: http (LISTEN)
httpd       4603 nobody    3u   IPv4   3326       TCP 192.168.111.22: http (LISTEN)
sshd        11519  root    4u   IPv4 1065327      TCP 210.29.192.22: ssh- > 192.168.18.32: 2442
(ESTABLISHED)
```

从以上输出中可以看到,lsof 列出了所有打开的端口以及哪个进程控制打开的端口。一定要知道每一个进程正在做什么以及它为什么打开端口。定期检查在系统上运行的进程列表,如果发现无法识别的进程,需要进行深入的调查。

4) 注意被更改过的文件

有人在入侵系统后,会试图更改系统文件,以便继续访问系统。这些可以将入侵者引入系统的文件被称为 rootkit,因为文件允许入侵者继续获得对 root 账号的访问。除了嗅探器程序外,入侵者还常用以下一些二进制的文件,如 ftpd、passwd、inetd、ps、login、

ssh 和 netstat 等。这些文件可以帮助入侵者维持访问的所有可执行文件。确定文件是否被替换的最佳方法是使用密码校验，最好在构建系统时对所有系统文件计算校验和，并且在为系统安装补丁程序时更新校验和。一定要确保将校验和放在安全的系统上，这样入侵者在更改文件时就无法更改校验和。如果怀疑系统受到攻击，则可以重新计算校验和进行比较。如果发现校验和不同，最好使用安装介质中的原始文件来进行替换。

**3. 掌握最新安全产品和技术**

作为一个系统管理员，必须时刻跟踪 Linux 安全技术的发展动向，并且适时采用更先进的 Linux 安全工具。目前国际上有许多有关 Linux 安全的研究和开发项目，目前至少有三个安全 Linux 项目已经启动，每个项目的目标都有自己的侧重点。

(1) 安全 Linux(SecureLinux)：安全 Linux(www.reseau.nl/securelinux)项目的目标是提供一个用于 Internet 服务器系统的安全的 Linux 分发。该项目管理者正寻求在这个产品中集成强大的密码和一些额外的 Web 服务器功能。既然它是在美国之外创建的，人们可望得到改进的密码安全而不会受到美国安全产品出口法律的限制。

(2) BastilleLinux：BastilleLinux(www.bastille-linux.org)项目寻求在 Linux 环境中建立一个类似 OpenBSD 的标准。该项目宣称的目标是为台式机创建一个安全的分发，使网络管理者可以不用担心用户的安全。

(3) 访问安全 Linux 邮件列表：现在有许多关于 Linux 安全的邮件列表，如 securedistros@nl.linux.org、Kha0s-dev@kha0s.org 等，经常访问这些邮件列表可以得到大量的安全信息。还有另一个通用的邮件列表是 security-audit@ferret.lmh.ox.ac.uk，它是专门讨论源代码的安全审计的。这个列表可能与其他的邮件列表有大量的重复，但如果想了解源代码审计和相关安全问题的话还是很值得一读的。

## 4.3 Windows 2000 Server、Windows Server 2003 的安全

Windows Server 2003 作为 Microsoft 新推出的服务器操作系统，继承了 Windows 2000/XP 的易用性和稳定性，提供了更高的硬件支持和更加强大的安全功能，是目前较为成熟的网络操作系统。Windows Server 2003 安全性相对于 Windows 2000 等有较大的提高，它改变了微软以往的安全哲学体系，它认为 Windows 2003 操作系统默认就应该是安全的。但是事实上，虽然默认安装的 Windows 2003 绝对比默认的安装 Windows NT 或 Windows 2000 安全许多，但是它还是存在着一些不足。所以，需要根据实际情况来对 Windows Server 2003 进行全面安全配置。在系统投入正式使用前，用户应在断开网络的情况下安装好操作系统，并进行一些设置，以便使系统更加符合具体的安全环境与安全需求。

### 4.3.1 安全基线的配置

在配置 Windows Server 2003 的时候，应该确定安全需求策略，并立即部署和执行这

些策略。实现这一目的最好的方法是创建一个安全基线(security baseline)。安全基线是文档和公认安全设置的清单。在大多数情况下,安全基线会随着服务器角色的不同而产生区别。因此,用户最好创建几个不同的基线,以便将它们应用到不同类型的服务器上。例如,可以为文件服务器制定一个基线,为域控制器制定另一个基线,并为 Web 服务器制定一个和前两者都不同的基线。

系统包含一个叫"安全配置与分析"的工具,这个工具让用户可以将服务器的当前安全策略与模板文件中的基线安全策略相比较。用户可以自行创建这些模板或是使用内建的安全模板。安全模板是一系列基于文本的 INF 文件,被保存在%SYSTEMROOT%\SECURITY\TEMPLATES 文件夹下。检查或更改这些模板最简单的方法是使用管理控制台(MMC)。在 RUN 提示下输入 MMC 命令后回车打开控制台。在控制台加载后,选择添加/删除管理单元命令,Windows 就会显示添加/删除管理单元列表。单击"添加"按钮,将会看到所有可用管理单元的列表,如图 4-1 所示。选择安全模板管理单元,接着依次单击添加、关闭和确认按钮。在安全模板管理单元加载后,就可以查看每一个安全模板了,如图 4-2 所示。在遍历控制台树的时候,会发现每个模板都模仿组策略的结构。模板一般以每个模板的用途来命名。




**图 4-1 添加安全基线**

如果正在安全配置一个文件服务器,建议从 securews 模板开始。在审查所有的模板设置时,会发现尽管模板能被用来让服务器更加安全,但是不一定能满足用户的需求。某些安全设置可能过于严格或过于松散。建议修改现有的设置,或创建一个全新的策略。在控制台中右击 C:\WINDOWS\ Security\Templates 文件夹并在目标菜单中选择新建模板命令,就可以轻轻松松地创建一个新的模板。在创建了符合需求的模板后,回到添加/删除管理单元对话框,添加一个安全配置与分析的管理单元。在这个管理单元




**图 4-2 添加的安全模板格式**

加载后，右击“安全配置与分析”图标，接着在快捷菜单中选择“打开数据库”命令，然后单击“打开”按钮，用户可以使用提供的名称来创建必要的数据库。接着，右击“安全配置与分析”图标并在快捷菜单中选择“导入模板”命令，将会看到所有可用模板的列表，选择包含安全策略设置的模板并单击打开。在模板被导入后，再次右击“安全配置与分析”图标并在快捷菜单中选择“现在就分析计算机”命令。Windows 将会提示写入错误日志的位置，输入文件路径后单击“确定”按钮。在这样的情况下，Windows 将比较服务器现有安全设置和模板文件里的设置。用户可以通过“安全配置与分析控制台”看到比较结果。每一条组策略设置显示了现有的设置和模板设置。在检查完差异列表的时候，就是执行基于模板安全策略的时候了。右击“安全配置与分析”图标并从快捷菜单中选择“现在就配置计算机”命令。这一工具将会立即修改计算机的安全策略，从而匹配模板策略。组策略实际上是层次化的，可以被应用到本地计算机级别、站点级别、域级别和 OU 级别。当用户实现基于模板的安全之时，修改的是计算机级别的组策略，其他的组策略不会受到直接影响。最终策略可能会反映变化，因为计算机策略设置被更高级别的策略所继承。

下面就详细介绍安全策略的配置，一般可以将安全配置策略设置分为本地安全策略设置和系统配置设置。

## 4.3.2 本地安全策略设置

本地安全策略的设置通过一个图形界面来配置，它本质上是一个修改注册表的前端界面，因此不需要再使用 regedit 来修改参数，具体位置可通过单击“控制面板”→“管理工具”→“本地安全策略”找到这个工具。这个工具非常强大，提供了对账户策略、本地策略、公钥策略、软件限制策略等的设置，如图 4-3 所示。

Windows 2003 系统提供了一些安全配置模板，可以使用它们来设置系统上的系统配置、本地安全策略和用户管理设置。如果用户对 Windows 2003 系统有足够的了解，并理解每一项更改可能给系统带来的影响，可以根据需要对其进行设置，如图 4-4 所示。下面先介绍一下安全策略管理中最基本的一些要素，对它的配置可以通过相应栏目的属性




图 4-3　本地安全策略管理器 GUI

进行设置。




图 4-4　配置示例

(1) 交互式登录：Windows 2003 提供了两种设置来定义显示给用户的登录信息，包括用户尝试登录时显示消息的文字及主题，目的是用于提醒登录用户进入的域。

(2) 关机时清理虚拟内存页面交换文件：在系统运行时，虚拟内存页面交换文件包含重要的系统信息，这些系统信息可能会包括加密的密钥或密码散列。所以，最好强制 Windows 2000/2003 在关机时清除系统的页面交换文件，使用“关机时清理虚拟内存页面交换文件”。

(3) 允许在未登录前关闭系统：这个选项需要禁用，用户不应该在没有登录时就关闭系统。

(4) 网络管理认证级别：网络认证系统是允许 Windows 2000/2003 服务器与 Windows 客户机一起工作的认证系统。它的认证模式比 Windows NT 或 Windows 2000 认证系统要简单。

(5) 对匿名连接的额外限制。

(6) 软件限制策略：用户可以定义默认的安全级别为 Unrestricted(未限制)或 Disallowed(未同意)。后者是比较好的安全级别，但这种限制过于严格，有时可能会影响操作。在运用时，需要做一些严格的测试。在设置了默认级别后，用户可以根据需要进行修改，为此创建针对具体的软件限制策略规定，可以基于软件做出下面的例外规定。

(1) 散列。

(2) 证书。

(3) 路径(包括 Registry 路径)。

(4) Internet 区。

软件限制策略的一个工作示例如下。

(1) 限制某类文件在电子邮件程序的电子邮件附件目录里运行。

(2) 限制某用户可以在终端服务器上运行哪些程序。

### 4.3.3 系统安全策略配置

在系统管理方面，主要讨论文件系统、网络系统、账户设置、服务包和补丁程序 4 个领域。作为一般性的原则，应该由机构的安全策略和系统配置要求来控制特定的设置。

#### 1. 文件系统的管理

NTFS 系统为一种高级的文件系统，提供了性能、安全、可靠性以及未在任何 FAT 格式版本中提供的高级功能。通过它可以实现任意文件及文件夹的加密和权限设置(这是最直观的安全设置了)，磁盘配额和压缩等高级功能。通过它还可以更好地利用磁盘空间，提高系统运行速度。自 Windows NT 系统以来，使用 NTFS 系统已经逐渐成了一种共识。NTFS 文件系统随 Microsoft Windows 的每个新版本而改进，而且 NTFS 的默认权限对于大多数组织已足够。如果用户在安装时不选用 NTFS 系统，那么后面的很多安全配置，如用户权限设置等都不能实现。所以，在 Windows 2003 上的文件系统默认设置成 NTFS。NTFS 具有一些新的个人权限，如下所示。

(1) 遍历文件夹/执行文件。

(2) 列举文件夹/读数据。

(3) 读属性/读扩展属性。

(4) 创建文件/写数据。

(5) 创建文件夹/附加数据。

(6) 写属性/写扩展属性。

(7) 读权限/更改权限。

NTFS 文件系统随 Microsoft Windows 每个新版本的改进而改进，而且 NTFS 的默认文件权限对于大多数情况而言已经足够了。管理员可以在组策略对象编辑器中配置

文件系统安全设置。将对默认文件系统安全设置的任何更改部署到大型组织之前，应在实验室环境中进行彻底的测试。在某些情况下，如果改动了文件权限，则可能需要完全重新构建受影响的计算机系统。

如果不打算使用“受限制的组”功能阻止 Power Users 组的成员或者打算启用“网络访问：让每个人(everyone)权限应用于匿名用户”设置，则需要应用可选权限。这些权限非常特定，它们将附加限制应用于某些可执行工具，具有提升特权的恶意用户可能使用这些工具来进一步破坏计算机或网络。这些更改不会影响系统卷的多个文件夹或根，但是以该方式更改权限非常危险，这样常常导致计算机不稳定。在将系统正式使用前，系统管理员需要了解最新的权限并查看关于文件和目录的权限结构，应该使用用户组来设置文件和共享资源的权限，这样可以更容易地管理文件的权限。

NTFS 分区支持文件级和文件夹级的 ACL，文件分配表(FAT)或 FAT32 文件系统不支持 ACL。FAT32 是 FAT 文件系统的一个版本，已更新为允许相当小的默认群集大小，并支持大于 2G 的硬盘。要转换成 NTFS 格式可以使用 NTFS 格式化每台服务器上的所有分区。使用转换实用程序将 FAT 分区转换为 NTFS 时应格外小心，转换实用程序会将转换的驱动器的 ACL 设置为“Everyone：完全控制”。

### 2. 网络系统的管理

与 Windows NT 相比，Windows 2000/2003 的网络有了较大的变化，除了标准的 Windows 端口(135、137 和 139)外，还增加了用于 Kerberos 的端口 88、用于 IP 上的 SMB 的端口 445、用于 Kerberos Kpasswd 的端口 464 以及用于 Internet 密钥交换的端口 500。这样，当用户希望从系统中删除 NetBIOS 时，则实际上必须禁止使用特定端口上的 Microsoft 网络文件和打开共享。在 Windows 2000/2003 维护着一个集中控制的用户数据库，活动目录结构使用了分层的概念，可以在其他组之上或之下创建组，可以将域分为具有本地控制的机构单位。

### 3. 账户设置与管理

在 Windows 2003 系统中，用户管理对于系统和机构的安全至关重要。在机构内部，应该确定每个新用户应具有的正确权限的正确程序。当发生人员变动时，应该具有保证员工不再能够访问本系统的程序。向系统中添加新用户时，一定要按照用户管理的过程进行。新用户要通过用户管理器添加到系统或者域中。和 Linux 系统一样，每个用户都应该有一个唯一的用户 ID 及他们自己的账户。如果两个用户需要相同的访问，则应该创建两个账户并将其放入同一个组。在任何情况下都不应该让多个用户使用相同的用户 ID。在用户设置结束后，需要设定初始密码，并且应该选定“用户下次登录时须更改密码”复选框，如图 4-5 所示。在创建了账户之后，必须将其添加到相应的组中，可以加入每一个单独的组，但标准的用户账户不应该是 Administrator 组的成员。

与向系统中添加用户一样，在删除用户时，管理员也必须按照用户管理过程来进行。当用户脱离机构时，应该立即禁用用户的账户，同时将其密码更改为完全随机的密码，这样可以防止该用户或其他人使用这个账户。如果用户拥有相应的文件和目录，应保持这




图 4-5 用户的添加与删除

个账户被禁用一段时间,以便相应的部门有足够的时间来处理这些文件。处理完毕后,可以将这个用户及其文件目录进行删除。Windows Server 2003 具有大量不能删除但可重命名的内置用户账户。Windows Server 2003 中的两个最为人熟知的内置账户为 Guest 和 Administrator。默认情况下,Guest 账户在成员服务器和域控制器上被禁用。此配置不可更改。许多恶意代码的变种在初次尝试破坏服务器时使用内置 Administrator 账户。因此,重命名内置 Administrator 账户和更改描述有助于防止试图使用此知名账户的攻击者对远程服务器进行破坏。近几年来,进行上述重命名配置的意义已经大大降低了,因为出现了很多新的攻击工具,这些工具通过指定内置 Administrator 账户的安全标识符(SID)来确定该账户的真实姓名,从而侵入服务器。SID 是用来唯一标识网络上的每个用户、用户组、计算机账户和登录会话的值。此内置账户的 SID 是不可更改的。不过,如果使用独特的名称来重命名 Administrator 账户,其所在的操作组就可以轻松监视针对该 Administrator 账户所进行的攻击尝试。完成下列步骤可保护域和服务器上众所周知的账户。

(1) 在每个域和服务器上,重命名 Administrator 和 Guest 账户,然后将其密码更改为长而复杂的值。

(2) 在每个服务器上使用不同的名称和密码。如果所有域和服务器使用同一个账户名和密码,则取得其中一台成员服务器访问权的攻击者就可以用相同的账户名和密码取得所有其他域和服务器的访问权。

(3) 将账户描述更改为不同于默认描述的内容,从而避免使用简单的账户标识。

(4) 将所做的任何更改记录在安全位置。

**注意:** 内置 Administrator 账户可通过组策略重命名。此设置不在基准策略中实施,因为每个组织都应为此账户选择一个独特的名称。

账户策略包括密码策略、账户锁定策略和 Kerberos 策略安全设置。密码策略提供了一种方法来设置高安全环境的复杂性和更改计划。账户锁定策略允许跟踪失败的密码登录尝试以便在必要时启动账户锁定。Kerberos 策略用于域用户账户，并确定与 Kerberos 身份验证协议相关的设置，如票证使用期限和强制。

1）密码策略

定期更改的复杂密码可以有效降低密码攻击成功的可能性。如图 4-6 所示，密码策略设置控制密码的复杂性和使用期限。利用在组策略对象编辑器中对以下位置中的密码策略设置进行配置。

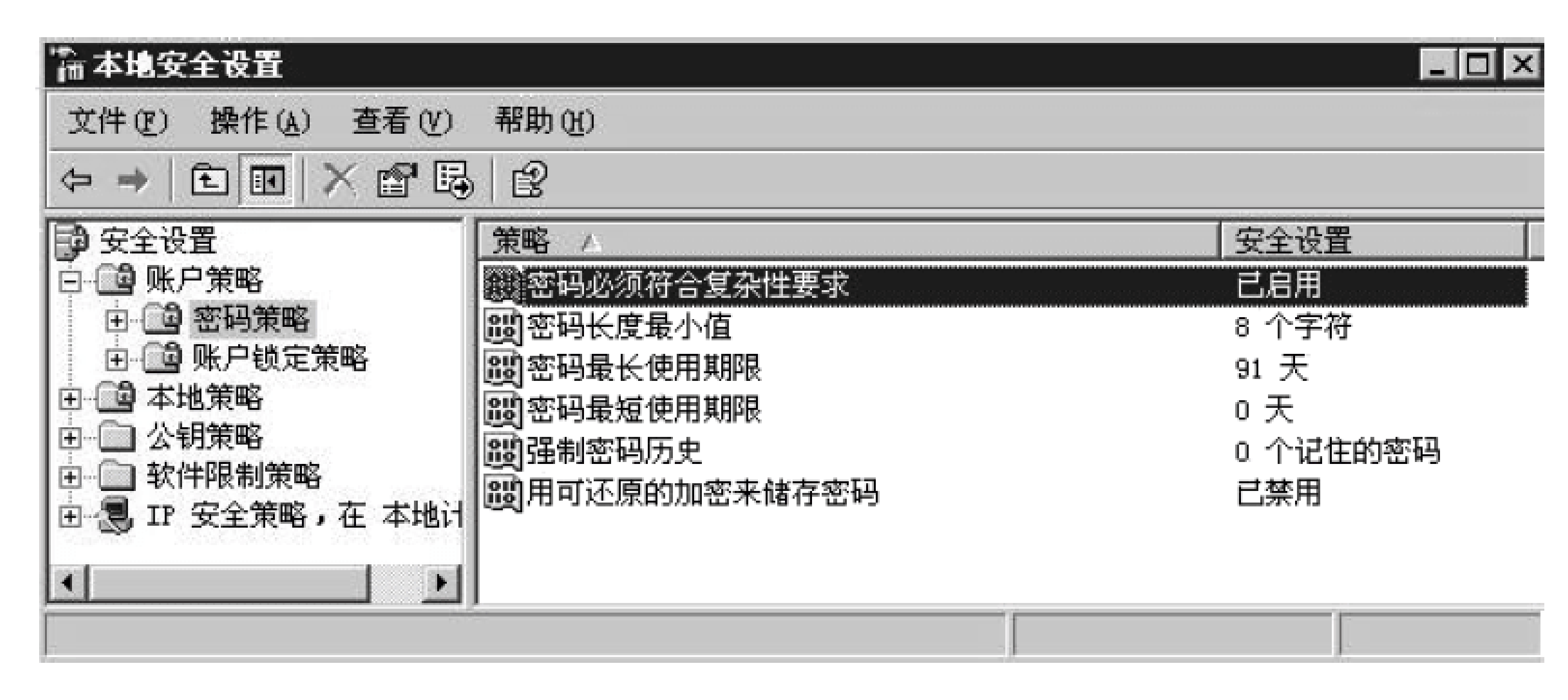



**图 4-6　使用本地安全设置密码策略**

(1) 强制密码历史：它有助于确保旧密码不会连续重新使用、常见的漏洞与密码重新使用相关联以及低值设置将允许用户持续循环使用数目很小的密码。此外，对于包括旧客户端的环境，此建议没有已知问题。要增强此策略设置的有效性，也可以配置“密码最短使用期限”设置以便密码无法被立即更改。这种组合使得用户很难重新使用旧密码，无论是偶然还是有意。

(2) 密码最长使用期限：默认值为 42 天。定期更改密码有助于防止密码遭破坏。若攻击者有足够的时间和计算功能，就能够破解大多数密码。密码更改越频繁，攻击者破解密码的时间就越少。

(3) 密码最短使用期限：默认值为 1 天。如果将此设置与“强制密码历史”设置中的类似低值相结合使用时，用户可以不断循环使用相同的密码。

(4) 密码长度最小值：用来确保密码至少具有指定个数的字符。此配置可针对常用词典和强力攻击提供相当强的防御功能。

(5) 密码必须符合复杂性要求：设置将检查所有新密码以确保它们符合安全性要求。不能对 Windows Server 2003 策略规则直接进行修改。实际上，可以设置包含 20 个或更多字符的密码，这样便于用户记忆，并且比八字符的密码更安全。因此，Microsoft 建议将“密码必须符合复杂性要求”设置配置为“已启用”。

(6) 用可还原的加密来储存密码：设置确定操作系统是否使用可逆加密来存储密码。它支持使用要求用户通过密码进行身份验证的协议的应用程序。如果启用此设置，会增加漏洞。建议此设置配置为“已禁用”，除非应用程序要求超过了保护密码信息的需要。

2）账户锁定策略

账户锁定策略指定时间段内多次登录尝试失败后锁定用户账户。允许尝试的次数和时间段基于为策略配置的值。Windows Server 2003 可跟踪登录尝试，而且服务器软件可以配置为通过在预设的登录失败次数后禁用账户来对潜在攻击做出响应。这些策略设置有助于保护用户密码，防止攻击者猜出密码，因此降低了网络攻击成功的可能性。用户可以使用组策略对象编辑器在下列位置对域组策略中的这些设置进行配置。

（1）账户锁定时间：设置在未锁定账户且用户可以尝试再次登录之前的时间长度。如果将“账户锁定时间”值设置为 0，则账户将保持锁定直到管理员将其解除锁定。

（2）账户锁定阈值：设置用户在账户被锁定之前可以尝试登录账户的次数。要避免锁定授权用户，请将“账户锁定阈值”设置配置为较高的数字。

（3）复位账户锁定计数器：确定在“账户锁定阈值”复位为 0 以及账户被解锁之前所必须经过的时间长度。如果没有复位账户锁定的策略设置，管理员必须手动解锁所有账户。相反，如果为此设置配置了合理的时间值，用户将会被锁定一段固定的时间，然后所有账户都会自动解锁。

3）用户权限分配策略加重

用户权限分配向用户和组提供组织中计算机的登录权限或特权。登录权限的一个示例是交互登录计算机的权限。特权的一个示例是关闭计算机的权限。这两种用户权限都由管理员作为计算机安全设置的一部分分配给单个用户或组。可以在 Windows Server 2003 中组策略对象编辑器的以下位置配置用户权限分配设置。

（1）从网络访问此计算机：此策略设置允许哪些用户和组通过网络连接到计算机。它是许多网络协议所需的，包括基于服务器消息块（SMB）的协议、NetBIOS、通用 Internet 文件系统（CIFS）、HTTP 和组件对象模型＋（COM＋）。

（2）以操作系统方式操作：此策略设置进程是否采用任何用户的标识，来获取对该用户被授权访问资源的访问权限。通常，只有低级别的身份验证服务才需要此用户权限。

（3）调整进程的内存配额：此策略设置用户是否可以调整可用于进程的最大内存量。它对于计算机优化非常有用，但可能会被滥用。攻击者可能会利用此用户权限来启动 DoS 攻击。

（4）允许在本地登录：此策略设置哪些用户可以交互登录指定的计算机。使用 Ctrl＋Alt＋Del 组合键启动登录要求用户具有此权限。具有此用户权限的任何账户都可以用于登录计算机的本地控制台。

（5）通过终端服务允许登录：此策略设置哪些用户或组有权作为终端服务客户端进行登录。

（6）备份文件和目录：此策略设置用户是否可以绕过文件和目录权限来备份计算机。仅当应用程序尝试使用备份实用程序（如 NTBACKUP. EXE）通过 NTFS 备份应用程序接口进行访问时，才会用到它。否则，应为正常的文件和目录权限。

（7）跳过遍历检查：此策略设置当用户在 NTFS 文件系统或注册表中浏览对象路径时是否可以通过文件夹，而不会被检查是否具有专门的“遍历文件夹”访问权限。用户权

限不允许用户列出文件夹的内容，它只允许用户遍历其目录。

(8) 更改系统时间：此策略设置哪些用户可以更改计算机内部时钟上的时间和日期。被分配了此用户权限的用户可以影响事件日志的外观，这将由计算机的内部时钟打上时间戳。如果计算机的时间被更改，日志将无法反映事件发生的实际时间。

**注意**：本地计算机和域控制器上之间的时间差异可能导致 Kerberos 身份验证协议发生问题，这可能使用户无法登录域或在登录之后无法获取授权来访问域资源。

(9) 创建页面文件：此策略设置用户是否可以创建和更改页面文件的大小。要执行此任务，用户必须在"性能选项"框(位于"系统属性"对话框的"高级"选项卡上)中为特定的驱动器指定页面文件大小。

(10) 创建标记对象：此策略设置进程是否可以创建令牌以及在进程使用 NtCreateToken()或其他令牌创建 API 时，进程可以使用哪个令牌获取任何本地资源的访问权限。

(11) 创建全局对象：此策略设置允许用户创建可供所有会话使用的全局对象。在没有被分配此用户权限的情况下，用户仍可以创建特定于其自身会话的对象。

(12) 创建永久共享对象：此策略设置用户是否可以在对象管理器中创建目录对象，这意味着他们可以创建共享文件夹、打印机和其他对象。对于扩展对象命名空间的内核模式组件，这非常有用，而且此类组件本来就具有此用户权限。因此，通常不必要专门向用户分配此用户权限。

(13) 调试程序：此策略设置哪些用户可以将调试程序附加到任何进程或内核。它提供对敏感和重要操作系统组件的完全访问权限。不要在生产环境中调试程序，除非是在极端情况下，例如，需要对测试环境中不能高效访问的业务关键型应用程序进行故障诊断。

(14) 拒绝从网络访问这台计算机：此策略设置哪些用户将不能通过网络来访问计算机。它拒绝许多网络协议，包括基于 SMB 的协议、NetBIOS、CIFS、HTTP 和 COM+。当用户账户受这两种设置的约束时，此策略设置将取代"从网络访问此计算机"用户权限。

(15) 拒绝作为批处理作业登录：此策略设置哪些账户无法作为批处理作业登录计算机。批处理作业不是批处理(.bat)文件，而是批处理队列工具。使用任务计划程序安排作业的账户需要此用户权限。"拒绝作为批处理作业登录"用户权限会覆盖"作为批处理作业登录"用户权限，后者可用于允许账户安排会过度消耗系统资源的作业。这种情况出现一次就会导致 DoS 条件。

(16) 拒绝作为服务登录：此策略设置是否可以在指定账户的上下文中启动服务。

(17) 拒绝本地登录：此策略设置用户是否可以从计算机直接登录。

(18) 通过终端服务拒绝登录：此策略设置用户是否可以作为终端服务客户端进行登录。在基准成员服务器加入到域环境后，不必使用本地账户从网络访问服务器。域账户可以访问服务器，以便执行管理和最终用户进程。

(19) 允许计算机和用户账户被信任以便用于委任：此策略设置用户是否可以更改 Active Directory 中用户或计算机对象上的"已为委派信任"设置。被分配了此用户权限

的用户或计算机还必须具有对象上账户控制标记的写入访问权限。滥用此用户权限可能导致对网络上其他用户的未经授权模拟。

(20) 从远程系统强制关机：此策略设置用户是否可以从网络上的远程位置关闭计算机。可以关闭计算机的任何用户均会造成 DoS 条件。因此，此用户权限应严格限制。

(21) 生成安全审核：此策略设置进程是否可以在安全日志中生成审核记录。因为安全日志可用于跟踪未经授权的访问，攻击者可能使用可以写入至安全日志的账户，将日志填满毫无意义的事件。如果将计算机配置为根据需要覆盖事件，攻击者可能使用此功能将他们的未经授权活动的证据删除。如果将计算机配置为在不能写入至安全日志时关闭，则攻击者可能使用此功能创建 DoS 条件。

(22) 身份验证后模拟客户端：此策略设置代表经过身份验证的用户运行的应用程序是否可以模拟客户端。如果此类型的模拟需要此用户权限，则未经授权的用户将无法说服客户端（如通过远程过程调用（RPC）或命名管道）连接到他们创建以模拟该客户端的服务。未经授权的用户可以使用此功能将其权限提升为管理或系统级别。

(23) 增加计划优先级：此策略设置用户是否可以提高进程的基本优先级。在优先级内提高相对优先级不是一个特权操作。随操作系统附带的管理工具不需要此用户权限，但软件开发工具可能需要。被分配了此用户权限的用户可以将进程的调度优先级提升至“实时”，为其他所有进程留下很少的处理时间，从而导致 DoS 条件。

(24) 装载和卸载设备驱动程序：此策略设置哪些用户可以动态加载和卸载设备驱动程序。如果新硬件的已签名驱动程序已经存在于计算机的 Driver.cab 文件中，则不需要此用户权限。设备驱动程序可以作为高特权代码运行。被分配了“装载和卸载设备驱动程序”用户权限的用户可以安装恶意代码，该恶意代码会伪装成设备驱动程序。管理员应格外小心，仅安装具有经过验证的数字签名的驱动程序。

(25) 内存中锁定页面：此策略设置进程是否可以将数据保留在物理内存中，这将阻止计算机将数据分页至磁盘上的虚拟内存。这种情况可能显著降低性能。被分配了此用户权限的用户可以将物理内存分配给几个进程，为其他进程留下很少或不留下任何随机存取存储器（RAM），可能导致 DoS 条件。

(26) 作为服务登录：此策略设置安全主体是否可以作为服务进行登录。服务可以配置为在 Local System、Local Service 或 Network Service 账户下运行，这些账户具有作为服务进行登录的内置权限。必须向在单独用户账户下运行的任何服务分配此用户权限。

(27) 管理审核和安全日志：此策略设置用户是否可以为文件、Active Directory 对象和注册表项等个别资源指定对象访问审核选项。此用户权限非常强大，应严密防护。具有此用户权限的任何用户都可以清除安全日志，并可能清除未经授权活动的重要证据。

(28) 修改固件环境值：此策略设置进程是否可以通过 API 或者用户是否可以通过“系统属性”更改计算机的环境变量。被分配了此用户权限的任何用户均可以配置硬件组件的设置，造成硬件组件故障，从而导致数据损坏或 DoS 条件。

(29) 执行卷维护任务：此策略设置非管理或远程用户是否可以管理卷或磁盘。被分配了此用户权限的用户可以删除卷，造成数据丢失或 DoS 条件。

(30) 配置单一进程：此策略设置哪些用户可以使用性能监视工具来监视非系统进程的性能。此用户权限表示适中的漏洞，具有此权限的攻击者可以监视计算机的性能，从而帮助确定他们想要直接攻击的重要进程。攻击者还可以确定计算机上运行的进程，以便识别要避免的对策(如防病毒软件、入侵检测系统或其他已登录计算机的用户)。

(31) 配置系统性能：此策略设置类似于前一设置。它确定用户是否可以监视系统进程的性能。此用户权限表示适中的漏洞，具有此特权的攻击者可以监视计算机的性能以帮助确定他们想要直接攻击的重要进程。攻击者还可以确定计算机上运行的进程，以便识别要避免的对策(如防病毒软件或入侵检测系统)。

(32) 从扩展坞中取出计算机：此策略设置便携式计算机的用户是否可以通过单击“开始”菜单上的“弹出 PC”来移除计算机。被分配了此用户权限的任何用户均可以从扩展坞中取出便携式计算机。

(33) 替换进程级别标记：此策略设置父进程是否可以替换与子进程相关联的访问令牌。

(34) 还原文件和目录：此策略设置哪些用户在他们还原备份的文件和目录时可以绕过文件、目录、注册表和其他永久对象权限。它还确定哪些用户可以将任何有效的安全主体设置为对象的所有者。

(35) 关闭系统：此策略设置哪些本地登录的用户可以使用“关闭”命令来关闭操作系统。由于滥用此功能可能导致 DoS 条件，因此，关闭域控制器的能力应限制于极少数的受信任管理员。即使关闭系统要求有登录到服务器的权限，也应谨慎处理允许关闭域控制器的账户和组。

(36) 同步目录服务数据：此策略设置进程是否可以读取目录中的所有对象和属性，而不管对象和属性是否受到保护。使用 LDAP 目录同步(Dirsync)服务时需要此用户权限。

(37) 取得文件或其他对象的所有权：此策略设置用户是否可以取得网络中任何安全对象的所有权，包括 Active Directory 对象、NTFS 文件系统 (NTFS) 文件、文件夹、打印机、注册表项、服务、进程以及线程等。

4) Kerberos 策略

Kerberos 策略用于域用户账户。这些策略确定与 Kerberos v5 身份验证协议相关的设置，如票证使用期限和强制。Kerberos 策略在本地计算机策略中不存在。如果减少 Kerberos 票证的使用期限，那么攻击者尝试窃取密码以模拟合法用户账户的风险将降低。但是，这些策略的维护需求将增加授权开销。在大多数环境中，不应更改这些策略的默认值。Kerberos 设置被包括在默认域策略中并在该策略中强制实施。

### 4. 服务包和补丁程序

有些网络已经具备了良好的边界安全措施，也普遍部署了病毒防御机制。但安全事件，特别是病毒的侵扰防不胜防，一方面是由于现有防御体系的缺陷，是由于现有的边界防御、基于签名的入侵检测和防病毒系统从原理上就决定了其不擅长对付基于漏洞进行感染的病毒。单单具备这些措施，还不足以遏制病毒的泛滥。另一方面也是由于基于漏

洞进行感染的病毒传播速度极快，以至于来不及采取措施，病毒就已经大规模爆发了。因此，对于一个网络而言，制定一个有效的 Windows 系统补丁管理措施，为客户段即时安装各种安全补丁和更新可以极大地增加企业内部的安全性。Microsoft 公司有时会提供一个集成的补丁程序包，用户可以下载安装。但更好的方式是 Microsoft Windows Server Update Services(WSUS)服务，它为在网络中管理更新提供一个全面的解决方案。WSUS 是设计用来大量精简 IT 系统在执行重大更新时的程序。通过使用 Windows Server 更新服务(WSUS)，管理员可以快速而可靠地将 Windows 2000 操作系统和更高版本、Office XP 和更高版本、Exchange Server 2003 以及 SQL Server 2000 的最新关键更新和安全更新部署到 Windows 2000 和更高版本的操作系统中。Windows 自动更新是 Windows 的一项功能，当适用于计算机的重要更新发布时，它会及时提醒下载和安装。使用自动更新可以在第一时间更新操作系统，修复系统漏洞，从而保护计算机安全，防止部分类型的病毒攻击。

### 5. 其他有关的安全配置问题

1) 终端服务的安全策略

在默认情况下，Windows Server 2003 提供了远程桌面，允许多达两个的远程会话。此外还有控制台会话。由于此功能允许用户从网络上的任何客户机对服务器进行远程管理，因此，保证其安全极为重要。为了尽可能保证安全，需要在终端服务配置管理单元中的具体连接的属性选项中进行设置。图 4-7 为终端服务配置管理单元的界面。




图 4-7 终端服务配置

(1) 加密级别：加密级别列举了可以选择的加密级别，用来保护在客户和服务器之间发送的数据。其中几个有关加密的选择说明如下。

① 低级别：使用 56 位加密对从客户端发送至服务器的数据进行加密。从服务器向客户端发送的数据不加密。

② 客户端兼容：使用客户端支持的最强密钥对客户端和服务器之间发送的数据进行加密。当终端服务器在包含混合或旧客户端的环境中运行时，请使用此级别。

③ 高级别：使用 128 位的密钥对数据加密。不支持这种级别加密的客户机无法连接(受推荐的加密级别)。使用 128 位加密的设置选项可防止攻击者使用数据包分析程序对终端服务进行窃听。某些旧版终端服务客户端不支持此高级加密。如果网络包含此类客户端，请设置连接加密级别以使用该客户端支持的最高加密级别发送和接收

数据。

(2) 登录设置：当客户机连接到终端服务器时，可以在此规定默认使用的登录信息，如图 4-8 所示。默认情况下使用客户机提供的登录信息。其他选项允许单一的用户账户用于所有的连接。最下面的选项要求即使提供了登录信息，用户也必须输入密码。

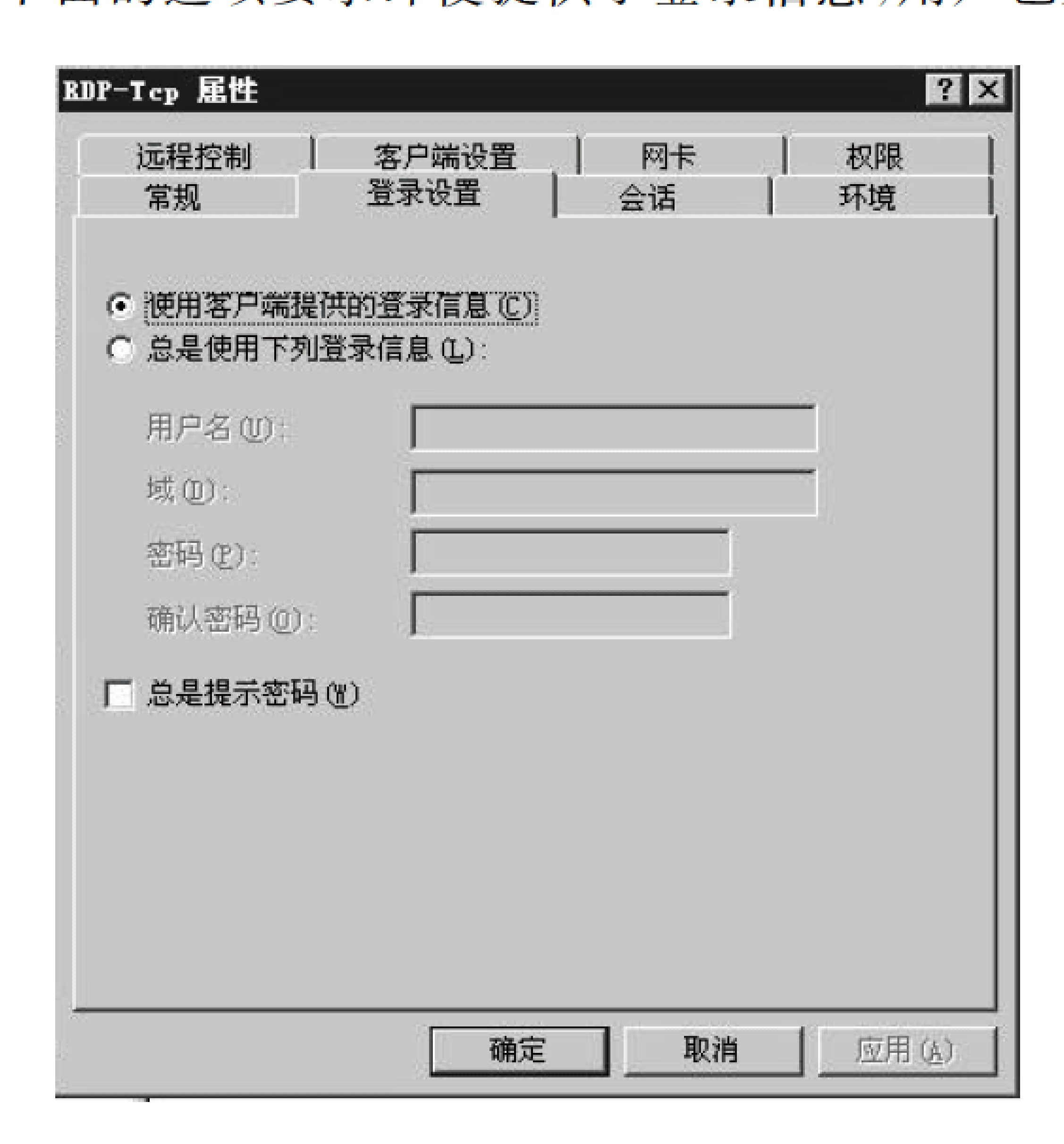



**图 4-8 Login Settings 选项卡**

2) NET Framework 配置

NET Framework Configuration 工具(如图 4-9 所示)的安全配置也需要说明一下，可以让用户对针对 NET Framework 1.1 设置代码访问安全策略。此工具可以保护和清除安装在此计算机上的托管组件。从安全的角度而言，此工具可以用来控制应用程序对受保护资源的访问。安全系统用 3 种策略级别来决定程序集的权限。

企业项针对整个企业的安全策略，计算机项应用于系统上运行的所有代码，用户项应用于当前登录的所有用户。这些策略分别进行评估，如组合实施策略，则代码就被授予最低的一组权限。任何 deny 权限都可以覆盖 allow 的权限。

3) 错误报告

此服务帮助 Microsoft 跟踪和解决错误。用户可以将此服务配置为给操作系统错误、Windows 组件错误或程序错误生成报告。Error Reporting 服务可通过 Internet 将此类错误报告给 Microsoft 或内部文件共享。虽然错误报告可能包含敏感或者甚至机密的数据，但是关于错误报告的 Microsoft 隐私策略将确保 Microsoft 不会滥用此类数据。但是，如果以明文 HTTP 传输数据，第三方就可以在 Internet 上截取并查看该数据。所以，“关闭 Windows 错误报告”设置可以控制错误报告服务是否传输任何数据。用户可以使用组策略对象编辑器中配置此策略设置。

4) 启用手动内存转储

Windows Server 2003 包含一种可用于中止计算机并生成 Memory.dmp 文件的功能。必须明确启用此功能，它可能并不适合于组织中的所有服务器。按照引用文件所述

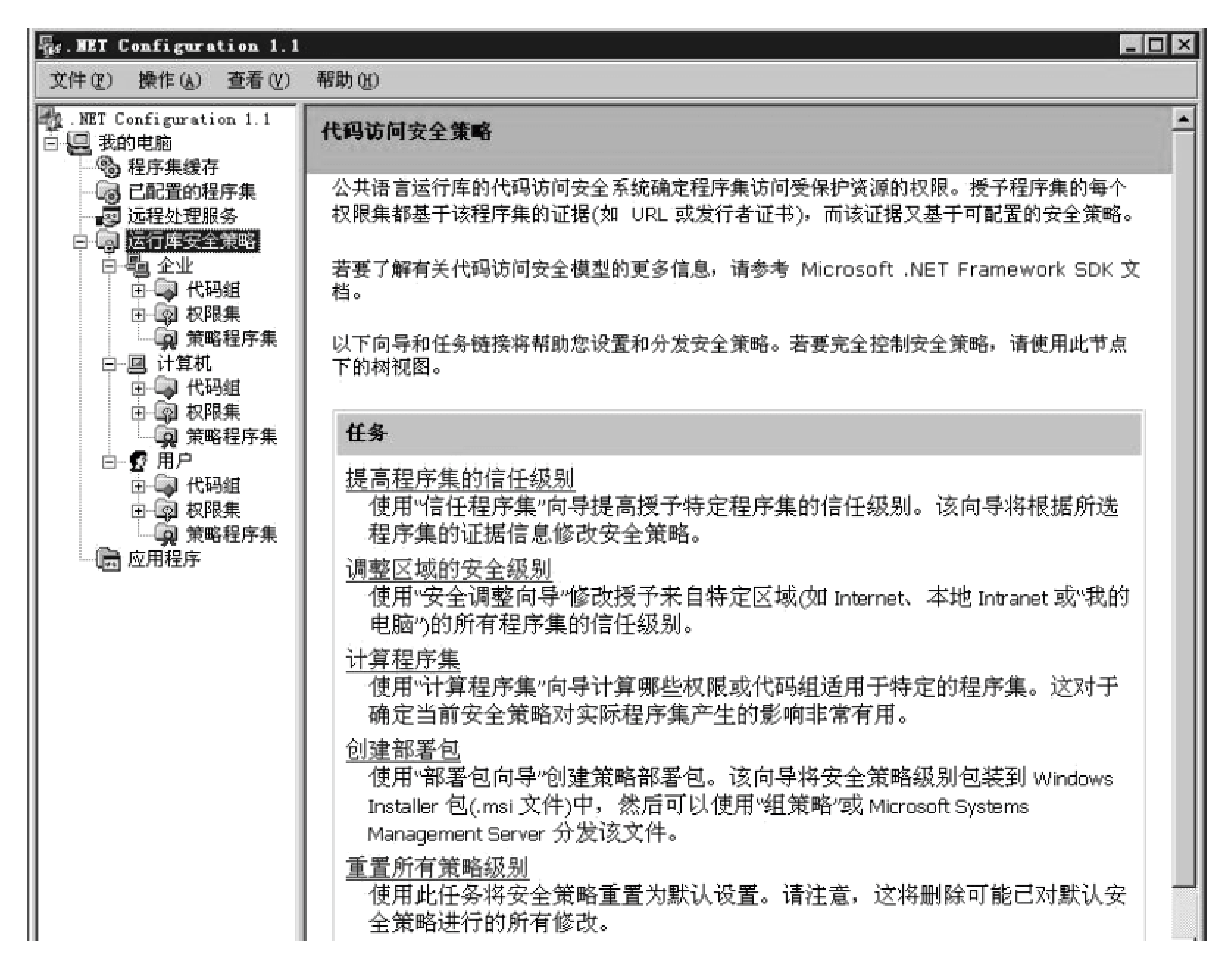



图 4-9 .NET Configuration 工具

将内存复制到磁盘时，敏感信息会被包括在 Memory.dmp 文件中。理想情况下，应禁止任何未经授权的人接触所有服务器。如果在其中生成内存转储文件的服务器面临物理破坏的风险，请确保在完成故障排除之后删除转储文件。

5）关闭不必要的服务

在系统上运行的代码越多，包含漏洞的可能性就越大。所以，一个重要安全策略是减少运行在服务器上的代码。这么做能在减少安全隐患的同时增强服务器的性能。在 Windows 2000 中，默认运行的服务有很多，但是有很大一部分服务在大多数环境中并派不上用场。而在 Windows Server 2003 中，微软关闭了大多数不是绝对必要的服务。即使如此，还是有一些有争议的服务默认运行。其中一个服务是分布式文件系统(DFS)服务。DFS 服务起初被设计简化用户的工作。DFS 允许管理员创建一个逻辑的区域，包含多个服务器或分区的资源。对于用户，所有这些分布式的资源存在于一个单一的文件夹中。如果不准备使用 DFS，需要让用户了解文件的确切路径。在某些环境下，这可能意味着更强的安全性。另一个这样的服务是文件复制服务(FRS)。FRS 被用来在服务器之间复制数据。它在域控制器上是强制的服务，因为它能够保持 SYSVOL 文件夹的同步。对于成员服务器来说，这个服务不是必须的，除非运行 DFS。如果文件服务器既不是域控制器，也不使用 DFS，建议禁用 FRS 服务。这么做会减少黑客在多个服务器间复制恶意文件的可能性。还有一个需要注意的服务是 Print Spooler 服务。该服务管理所有的本地和网络打印请求，并在这些请求下控制所有的打印工作。所有的打印操作都离不开这个服务，它也是默认被启用的。不是每个服务器都需要打印功能，除非服务器的角色是打印服务器，应该禁用这个服务。Print Spooler 是最危险的 Windows 组件之一，有不计其数的木马替换其可执行文件。这类攻击的动机是因为它是系统级的服务，因此

拥有很高的特权。因此，任何侵入它的木马能够获得这些高级别的特权。为了防止此类攻击，还是要关掉这个服务。

### 4.3.4 系统安全日常管理

在系统安装结束后，系统将开始提供相应的网络应用服务。在日常操作中，管理员的安全思想同样很重要。系统管理员在日常工作中需要做一些工作，以提高发现潜在的安全问题的能力。

**1. 应用 secedit 工具**

这是 Windows 2000/2003 内置的一个安全策略管理工具，主要利用它来分析正在讨论的系统策略并与所提出的策略进行比较，分析更改正在讨论的系统策略，以使其符合所提出的策略。可以使用 secedit 对运行在 Windows 2000/2003 系统上的现有策略与系统应该使用的策略进行比较，具体的操作是在命令行提示符下输入以下命令。

```
Secedit /analyze [/DB filename]- [/CFG filename ] [/log filename] [/verbose] [/quiet]
```

它提供以下参数以供选择。

(1) / DB 文件名　指定到达数据库文件的路径，该数据库中包含有分析的存储配置。如果文件名指定了一个新文件，则必须使用/CFG 参数。

(2) /CFG 文件名　指定到达安全模板的路径，该模板将被导入数据库中。如果不使用参数，则使用存储在数据库中的配置。

(3) /log 文件名　指定到达将由该命令创建的日志文件的路径。日志文件包括在分析过程中找到的所有信息。

(4) /verbose　告诉 secedit 在运行时提供详细情况。

(5) /quiet　告诉 secedit 在运行时不向屏幕提供输出。

运行完成之后，应该分析日志文件，以确定系统是否符合机构的策略。另外，secedit 可以用来配置系统，用来在系统中强制使用特定的安全配置，这个操作的命令语法如下。

```
secedit /configure [/DB filename] [/CFG filename ] [/overwrite] [/areas areal area2...] [/log
filename] [/verbose] [/quiet]
```

它提供以下参数以供选择。

(1) /DB 文件名　指定包含要使用模板的数据文件的路径。

(2) /CFG 文件名　指定到达一个安全模板的路径，可以将该安全模板导入数据库，然后应用于系统。

(3) /overwrite　指定由/CFG 命令标识的安全模板中的策略覆盖数据库中的策略。

(4) /areas 指定将要应用于系统的模板的安全区域。这些区域可以是 Securitypolicy、Group_mgmt、User_rights、Regkeys、Filestore、Services 等。如果没有指定区域，则默认为所有区域。

(5) /log 文件名　指定到达将由该命令创建的日志文件的路径。

(6) /verbose 告诉 secedit 在运行时提供详细的情况。

(7) /quiet 告诉 secedit 在运行时不向屏幕提供输入。

secedit 还可以验证一个安全配置文件,这种验证可以保证文件的语法是正确的,执行这种操作的命令如下。

```
secedit /validate filename
```

secedit 也可以向系统注入一个安全策略,用于确保系统使用的是正确的安全策略。具体命令如下。

```
setedit /refreshpolicy [machine_policy or user_policy] [/enforce]
```

它可以提供以下参数。

(1) machine_policy 指定应该刷新的用于本地计算机的安全策略。

(2) user_policy 指定应该刷新的当前登录到系统上的本地用户的安全设置。

(3) /enforce 指定即使没有改变也刷新的策略。

**2. 系统审核策略**

管理员应该创建审核策略以定义要报告哪些安全事件,并记录指定事件类别中的用户或计算机活动。管理员可以监视与安全相关的活动,例如,是谁访问了对象,用户是否登录计算机或从计算机注销,或者是否对审核策略设置进行了更改。在实施审核策略之前,必须确定环境所要审核的事件类别。管理员为事件类别选择的审核设置定义了组织的审核策略。为特定事件类别定义审核设置时,管理员可以创建适合组织的安全需要的审核策略。如果不存在审核策略,就很难确定安全事件中所发生的活动。但是,如果审核设置的配置导致许多授权活动都生成事件,则安全日志将被无用的数据填满。

通常,故障日志所提供的信息量比成功日志要大得多,因为故障往往指示错误。例如,用户成功登录计算机通常会被视为是正常的。但是,如果有人尝试登录计算机失败多次,这可能表明他尝试使用其他人的账户凭据来侵入该计算机。事件日志记录在计算机上发生的事件。在 Microsoft Windows 2003 操作系统中,有适用于应用程序、安全事件和系统事件的单独事件日志。安全日志记录审核事件。组策略的事件日志容器用于定义与应用程序、安全和系统事件日志有关的属性,例如,最大日志文件大小、对每个日志的访问权限,以及保留设置和方法。

在实施审核策略之前,应该确定它们将如何收集、组织和分析数据。如果没有利用计划,那么即使审核数据非常多,也没有什么价值。此外,在审核计算机网络时,性能也会受到影响。设置给定组合的影响在最终用户计算机上可忽略,但是在繁忙的服务器上的影响就相当明显。因此,在用户的应用环境中部署新的审核设置之前,应该测试性能是否将受到影响。这些操作可以在 Windows Server 2003 中组策略对象编辑器的以下位置配置审核策略设置值。

(1) 审核账户登录事件:此策略设置是否审核从另一台验证该账户的计算机登录或注销的用户的每个实例。对域控制器上的域用户账户进行身份验证将生成账户登录事件,该事件记录在域控制器的安全日志中。对本地计算机上的本地用户进行身份验证将

生成登录事件，该事件记录在本地安全日志中。不会记录任何账户注销事件。此策略设置记录在安全日志中的重要安全事件。如果要创建自定义警报以便监视任何软件包（例如，Microsoft Operations Manager，MOM），这些事件ID就非常有用。

（2）审核账户管理：此策略设置是否对计算机上的各个账户管理事件进行审核。账户管理事件的示例包括创建、更改或删除用户账户或组，重命名、禁用或启用用户账户，设置或更改密码。管理员需要能够确定谁创建、修改或删除了域和本地账户。未授权的更改有可能表明是由于不了解如何遵循组织策略的管理员做出的错误更改，但也可能表明了存在蓄意攻击。例如，账户管理失败事件往往表明低级别管理员或者破坏低级别管理员的账户的攻击者企图提升其特权。日志可以帮助管理员确定攻击者修改和创建了哪些账户。此策略设置记录在安全日志中的重要安全事件。如果要创建自定义警报以便监视任何软件包，这些事件ID就非常有用。

（3）审核登录事件：此策略设置是否审核登录计算机或从计算机注销的用户的每个实例。“审核登录事件”设置将在域控制器上生成记录以监视域账户活动，并在本地计算机上生成记录以监视本地账户活动。如果将“审核登录事件”设置配置为“无审核”，那么要确定组织中哪些用户已登录或尝试登录计算机就非常困难或不可能。如果在域成员上启用“审核登录事件”设置的“成功”值，那么每当某人登录网络时均将生成一个事件，而不管账户在网络上的驻留位置。如果用户登录到本地账户，并且“审核账户登录事件”设置为“已启用”，则用户登录会生成两个事件。如果用户不修改此策略设置的默认值，那么在发生安全事件后，就没有可用的审核记录证明。

（4）审核对象访问：就其自身而言，本策略设置不会导致任何事件被审核。“审核对象访问”设置在用户访问具有指定的系统访问控制列表（SACL）的对象（例如，文件、文件夹、注册表项或打印机）时是否要审核事件。SACL由访问控制项（ACE）组成。每个ACE包含三部分信息：审核的安全主体（用户、计算机或组）；要审核的特定访问类型（称为访问掩码）以及一个标记，表示是审核失败的访问事件，还是审核成功的访问事件或两者全部都进行审核。如果将“审核对象访问”设置配置为记录“成功”值，那么每当用户成功使用指定的SACL访问对象之后，将生成审核项。如果将此策略设置配置为记录“失败”值，那么每当用户尝试使用指定的SACL访问对象失败之后，将生成审核项。在配置SACL之后，应该只定义需要启用的操作。例如，用户可能需要针对可执行文件启用“写入和附加数据”审核设置，以跟踪它们何时被更改或替换，因为计算机病毒、蠕虫和特洛伊木马通常都是以可执行文件为目标的。同样，可能需要跟踪访问或更改敏感文档的时间。

（5）审核策略更改：此策略设置是否审核对用户权限分配策略、信任策略或审核策略自身所做的更改的每个事件。如果将“审核策略更改”设置为记录“成功”值，那么每当成功更改用户权限分配策略、信任策略或审核策略之后，将生成一个审核项。如果将此策略设置为记录“失败”值，那么每当更改用户权限分配策略、信任策略或审核策略失败之后，将生成一个审核项。建议设置允许用户查看攻击者试图提升的任何账户特权，例如，他们尝试添加“调试程序”特权或“备份文件和目录”特权。

（6）审核特权使用：此策略设置是否要审核用户权限的各项活动。如果将“审核特

权使用”设置为记录“成功”值,则每当成功执行用户权限时,就会生成一个审核项。如果将此策略设置为记录“失败”值,则每当执行用户权限失败时,就会生成一个审核项。执行以下用户权限之后不会生成审核,即使用户配置“审核特权使用”设置,因为这些用户权限将生成许多事件并记录在安全日志中。如果审核这些用户权限,就会影响用户的计算机的性能。这些用户权限包括跳过遍历检查、调试程序、创建标记对象、替换进程级令牌、生成安全审核、备份文件和目录、还原文件和目录。

**注意**:如果用户希望审核这些用户权限,则必须启用组策略中的“审核:对备份和还原权限的使用进行审核”安全选项。

(7) 审核过程跟踪:此策略设置是否审核事件的详细跟踪信息,如程序激活、进程退出、句柄复制和间接对象访问等。如果将此策略设置为记录“成功”值,则每当被跟踪的进程成功时,就会生成一个审核项。如果将此策略设置为记录“失败”值,则每当被跟踪的进程失败时,就会生成一个审核项。“审核过程跟踪”设置将生成大量的事件,因此,通常被配置为“无审核”,这种情况与本指南定义的所有三种环境的基准策略中的情况类似。但是,此策略设置在事件响应期间可能非常实用,因为它提供有关启动进程的详细日志以及每个进程的启动时间。

(8) 审核系统事件:此策略设置在用户重新启动、关闭计算机或者发生影响计算机的安全性或安全日志的事件时是否需要审核。如果用户将此策略设置为记录“成功”值,则在系统事件成功执行时,将生成一个审核项。如果用户将此策略设置为记录“失败”值,则在尝试系统事件失败时,将生成一个审核项。下表包括此设置的最有用的成功事件。

### 3. 日志文件的设置

事件日志记录计算机上的事件,而安全日志记录审核事件。使用组策略的事件日志容器来定义应用程序、安全和系统事件日志的属性,例如,最大日志文件大小、对每个日志的访问权限以及保留设置和方法。应用程序、安全性和系统事件日志的设置在 MSBP 中配置,并应用于域中的所有成员服务器。其主要包括以下几个方面。

(1) 应用程序日志大小最大值:此策略设置应用程序事件日志(最大容量为 4GB)大小的最大值。然而,不建议使用此大小,因为内存碎片风险可导致性能降低及事件日志记录不可靠。根据平台功能及应用程序相关事件历史记录的需要,对应用程序日志大小的要求有所不同。在本书定义的所有三种环境的基准策略中,“应用程序日志大小最大值”设置被配置为默认值 16 384KB。

(2) 安全日志最大值:此策略设置安全事件日志(最大容量为 4GB)大小的最大值。在域控制器和独立服务器上安全日志的大小应至少配置为 80MB,这应该足以存储足够的执行审核信息。如何为其他计算机配置此策略设置取决于许多因素,包括检查日志的频率、可用磁盘空间等。在本书定义的所有三种环境的基准策略中,“安全日志最大值”安全设置被配置为 81 920KB。

(3) 系统日志大小最大值:该策略设置最大的系统事件日志,最大容量超过 4GB 大小。然而,不建议使用此大小,因为内存碎片风险可导致性能降低及事件日志记录不可

靠。对系统日志大小的要求各不相同,取决于平台功能和历史记录的需要。在本书定义的所有三种环境的基准策略中,“系统日志大小最大值”设置被配置为默认值 16 384KB。

(4) 限制本地来宾组访问应用程序日志:此策略设置是否拒绝来宾组访问应用程序事件日志。Windows Server 2003 SP1 默认情况下,在所有计算机上都禁止来宾组访问。因此,此策略设置对使用默认配置的计算机没有实际影响。但是由于此配置被视为无负面影响的纵深防御措施,因此,在本书定义的所有三种环境的基准策略中,“限制本地来宾组访问应用程序日志”设置应被配置为“已启用”。

(5) 限制本地来宾组访问安全日志:此策略设置是否拒绝来宾组访问安全事件日志。用户必须被分配了“管理审核和安全日志”用户权限(本指导中未定义),才能访问安全日志。因此,此策略设置对使用默认配置的计算机没有实际影响。但是由于此配置被视为无负面影响的纵深防御措施,因此,在本书定义的所有三种环境的基准策略中,“限制本地来宾组访问安全日志”设置被配置为“已启用”。

(6) 限制本地来宾组访问系统日志:此策略设置是否拒绝来宾组访问系统事件日志。在 Windows Server 2003 SP1 默认情况下,在所有计算机上都禁止来宾组访问。因此,此策略设置对使用默认配置的计算机没有实际影响。但是由于此配置被视为无负面影响的纵深防御措施,因此,在本书定义的所有三种环境的基准策略中,“限制本地来宾组访问系统日志”设置被配置为“已启用”。

(7) 应用程序日志保留方法:此策略设置应用程序日志的“包装”方法。如果历史事件为辩论或故障排除之所需,则必须定期存档应用程序日志。如果按需要覆盖事件,日志将始终存储最新的事件,此配置会导致历史数据丢失。

(8) 安全日志的保留方法:该策略设置安全日志的环绕方法。如果历史事件为辩论或故障排除之所需,则必须定期存档安全日志。如果按需要覆盖事件,日志将始终存储最新的事件,此配置会导致历史数据丢失。

(9) 系统日志保留方法:该策略设置系统日志的环绕方法。如果历史事件为故障排除所需要,则必须定期存档日志。如果按需要覆盖事件,日志将始终存储最新的事件,此配置会导致历史数据丢失。

#### 4. 查找可疑迹象

在 Windows 系统的使用过程中,在设置了相应的安全策略后,还需要对系统的日常运行进行检查,及时发现系统可能存在的不良攻击。在进行系统检查时,需要注意下面几种情况。

1) 访问失败记录

访问失败可能表明授权用户试图访问敏感文件。一次的失败是无心之过,但如果发现一个用户对文件和目录拥有大量的访问失败记录,就需要引起高度警惕,查找原因。在安全事件日志中提供了失败的记录,它并不能构成某人未经授权就试图访问信息的证据。这些日志消息可以由用户不知道的访问企图进程产生,也可能由其他一些使用用户账户或系统的人产生。所以,不能单靠日志的记录就来判断某个人就有不良企图,还需要结合其他的证据进行判断。

2）日志文件缺失

在启用了审核并且正在运行的 Windows 2003 系统中，事件日志永远不会是空白的。许多有经验的入侵者会在进入系统后清空日志文件，以隐藏行为踪迹。如果发现空白的日志文件，就应该立即假定系统出现异常，并调查日志空白的原因。最近出现了一些允许入侵者修改日志文件中特定条目的工具，如果入侵者试图这样做，则在日志文件中发现空缺，要找出空缺，只需查看比一般时间间隔要长的日志条目的时间间隔即可。如果看到长时间的空缺，则应查明原因。

3）不明进程

大量的进程都在 Windows 系统上运行，一些进程容易识别，而另一些进程则不容量识别。查看任务管理器，可以看到运行的进程以及它们对 CPU 及内存的使用状况。系统管理员应改定期查看任务管理器，以了解是否有未知的进程在运行。CMD 进程是一个需要查看的好例子。CMD 进程是命令提示符或 DOS 窗口。如果它正在运行，则在屏幕上应出现一个窗口。在某些情况下，入侵者会启动 CMD 进程，以便在系统上执行其他操作，这是系统上存在不正常事件的一个明显迹象。

4）强力破解行动

如果有人通过手工或使用工具试图猜测账户密码，那么安全事件日志将包含表明登录的失败的条目。此外，如果将系统配置为在几次登录失败后锁定账户，则还会显示锁定账户的数量。安全事件日志中的失败登录企图信息会提供这种企图的源工作站的名称。应该从这台工作站开始调查一下，以确定出现登录失败的原因。调查类型应该由企图的来源决定，并根据来源的不同采取不同的措施。

另外，要配置一个安全的 Windows Server 2003 操作系统，理解服务器角色绝对是安全进程中不可或缺的一步。Windows Server 可以被配置为多种角色，它可以作为域控制器、成员服务器、基础设施服务器、文件服务器、打印服务器、IIS 服务器、IAS 服务器、终端服务器等。一个服务器甚至可以被配置为上述角色的组合。每种服务器角色都有相应的安全需求。例如，如果服务器将作为 IIS 服务器，那么需要开启 IIS 服务。然而，如果将服务器作为独立的文件或者打印服务器，启用 IIS 服务则会带来巨大的安全隐患。没有一种配置能解决所有的安全问题，服务器的安全应该随着服务器角色和服务器环境的改变而改变。

### 4.3.5 安全技巧

#### 1. 初级技巧

1）物理安全

服务器应该安放在安装了监视器的隔离房间内，并且监视器要保留 15 天以上的摄像记录。另外，机箱、磁盘、电脑桌抽屉都要上锁以确保旁人即使进入房间也无法使用，电脑钥匙要放在另外的安全的地方。

2）停掉 guest 账号

在计算机管理的用户里面把 guest 账号停用掉，任何时候都不允许 guest 账号登录

系统。为了保险起见，最好给 guest 加一个复杂的密码。可以打开记事本，在里面输入一串包含特殊字符、数字和字母的长字符串，然后把它作为 guest 账号的密码拷进去。

3）限制不必要的用户数量

去掉所有的 duplicate user 账户、测试用账户、共享账号和普通部门账号等。用户组策略设置相应权限，并且经常检查系统的账户，删除已经不在使用的账户。这些账户很多时候都是黑客们入侵系统的突破口。系统的账户越多，黑客们得到合法用户的权限可能性一般也就越大。国内的 Windows 2000/2003 主机，如果系统账户数超过 10 个，一般都能找出一两个弱密码账户来。

4）创建 2 个管理员用账号

虽然这点看上去和上面那点有些矛盾，但事实是服从上面的规则的。创建一个一般权限账号用来收信以及处理一些日常事务，另一个拥有 Administrators 权限的账户只在需要的时候使用。可以让管理员使用“RunAS”命令来执行一些需要特权才能做的工作，以方便管理。

5）把系统 administrator 账号改名

大家都知道 Windows 2000/2003 的 administrator 账号是不能被停用的，这意味着别人可以一遍又一遍地尝试这个账户的密码。把 administrator 账户改名可以有效地防止这一点。当然，请不要使用 admini 之类的名字，改了等于没改，尽量把它伪装成普通用户，比如改成 guestone。

6）创建一个陷阱账号

什么是陷阱账号？创建一个名为 administrator 的本地账户，把它的权限设置成最低，什么事也干不了的那种，并且加上一个超过 10 位的超级复杂密码。这样可以让那些 Scripts 忙上一段时间，借此发现它们的入侵企图。或者在它的 loginsc Scripts 上面做点手脚。

7）把共享文件的权限从 everyone 组改成“授权用户”

everyone 在 Windows 2000 中意味任何有权进入网络的用户都能够获得这些共享资料。任何时候都不要把共享文件的用户设置成 everyone 组，包括打印共享。默认的共享就是 everyone 组的，一定不要忘了改。

8）使用安全密码

一个好的密码对于网络是非常重要的，但是它是最容易被忽略的。前面所说的也许已经可以证明这一点了。一些公司的管理员创建账号时，往往用公司名、计算机名或者一些别的一猜就中的东西作用户名，然后又把这些账户的密码设置得太简单，比如 welcome、i love you、letmain 或者和用户名相同等。这样的账户应该要求用户首次登录的时候更改成复杂的密码，还要注意经常更改密码。在安全期内无法破解出来的密码就是好密码，也就是说如果人家得到了密码文档，必须花 43 天或者更长的时间才能破解出来，而密码策略是 42 天必须改密码。

9）设置屏幕保护密码

这个很简单也很有必要，设置屏幕保护密码也是防止内部人员破坏服务器的一个屏障。注意不要使用 OpenGL 和一些复杂的屏幕保护程序，比较浪费系统资源，让他黑屏就可以了。还有一点，所有系统用户所使用的机器也最好加上屏幕保护密码。

10）使用NTFS格式分区

把服务器的所有分区都改成NTFS格式。NTFS文件系统要比FAT、FAT32的文件系统安全得多。

11）运行防毒软件

在Windows 2000/2003服务器上安装防毒软件，其实这一点非常重要。一些好的杀毒软件不仅能杀掉一些著名的病毒，还能查杀大量木马和后门程序。这样的话，黑客们使用的那些有名的木马就毫无用武之地了。还有，不要忘了经常升级病毒库。

12）保障备份盘的安全

一旦系统资料被破坏，备份盘将是恢复资料的唯一途径。备份完资料后要把备份盘放在安全的地方。千万别把资料备份在同台服务器。那样的话，还不如不备份。

### 2. 中级技巧

1）利用Windows 2000/2003的安全配置工具来配置策略

微软提供了一套的基于MCC（管理控制台）安全配置和分析工具，利用它们可以很方便地配置服务器以满足需求。具体内容请参考微软主页。

2）关闭不必要的服务

Windows 2000/2003的Terminal services（终端服务）、IIS和RAS都可能给系统带来安全漏洞。为了能够在远程方便地管理服务器，很多机器的终端服务都是开着的，要确认已经正确地配置了终端服务。有些恶意的程序也能以服务方式悄悄地运行，要留意服务器上面开启的所有服务。中期性（每天）地检查它们。下面是C2级别安装的默认服务。

```
Computer  Browser  Service  TCP/IP  NetBIOS  Helper
Microsoft DNS server Spooler
NTLM SSP server
RPC Locator WINS
RPC service Workstation
Netlogon Event log
```

3）关闭不必要的端口

关闭端口意味着减少功能，在安全和功能上面需要进行协调。如果服务器安装在防火墙的后面，危险性会少些。但是，永远不要认为就可以高枕无忧了。用端口扫描器扫描系统所开放的端口，确定开放了哪些服务是黑客入侵你的系统的第一步。在system32\drivers\etc下的services文件中有知名端口和服务的对照表可供参考。具体方法是选择“网上邻居”→“属性”→“本地连接”→“属性”设置internet协议中的TCP/IP“属性”命令打开TCP/IP筛选，添加需要的TCP和UDP协议即可。

4）打开审核策略

开启安全审核是Windows 2000/2003最基本的入侵检测方法。当有人尝试对你的系统进行某种方式（如尝试用户密码、改变账户策略、未经许可的文件访问等）入侵的时候，都会被安全审核记录下来。很多的管理员在系统被入侵了几个月都不知道，直到系

统遭到破坏。下面的这些审核是必须开启的，其他的可以根据需要增加。

策略设置。

审核系统登录事件　成功，失败

审核账户管理　成功，失败

审核登录事件　成功，失败

审核对象访问　成功

审核策略更改　成功，失败

审核特权使用　成功，失败

审核系统事件　成功，失败

5）开启密码策略

策略设置。

密码复杂性要求　启用

密码长度最小值　6 位

强制密码历史　5 次

强制密码历史　42 天

6）开启账户策略

策略设置。

复位账户锁定计数器　20 分钟

账户锁定时间　20 分钟

账户锁定数值　3 次

7）设定安全记录的访问权限

安全记录在默认情况下是没有保护的，把它设置成只有 Administrator 和系统账户才有权访问。

8）把敏感文件存放在另外的文件服务器中

虽然现在服务器的硬盘容量都很大，但是还是应该考虑是否有必要把一些重要的用户数据（文件、数据表、项目文件等）存放在另外一个安全的服务器中，并且经常备份它们。

9）不让系统显示上次登录的用户名

默认情况下，终端服务接入服务器时，登录对话框中会显示上次登录的账户名，本地的登录对话框也是一样。这使得别人可以很容易地得到系统的一些用户名，进而进行密码猜测。修改注册表可以不让对话框里显示上次登录的用户名，具体内容如下。

```
HKLMS\software\Microsoft\Windows NT\Current Version\Winlogon\DontDisplayLastUser-Name
```

把 REG_SZ 的键值改成 1。如果没有，需要建立一个。

10）禁止建立空连接

默认情况下，任何用户可以通过空连接连上服务器，进而枚举账号猜测密码。可以通过修改注册表来禁止建立空连接，将 HKLM\System\CurruntControlSet\Control\LSA\RestrictAnonymous 的值改成 1 即可。

11）到微软公司网站下载最新的补丁程序

很多网络管理员没有访问安全站点的习惯，以至于一些漏洞都出了很久了，还放着服务器的漏洞不补。谁也不敢保证数百万行以上代码的 Windows 2000/2003 没有一点安全漏洞。经常访问微软和一些安全站点，下载最新的 service pack 和漏洞补丁，是保障服务器长久安全的唯一方法。

### 3. 高级技巧

1）关闭 DirectDraw

这是 C2 级安全标准对视频卡和内存的要求。关闭 DirectDraw 可能对一些需要用到 DirectX 的程序有影响（比如游戏），但是对于绝大多数的商业站点都应该是没有影响的。修改注册表，将 HKLM\SYSTEM\Cur rentControlSet\Control\GraphicsDrivers\DCI 的 Timeout 值改为 0 即可。

2）关闭默认共享

从 Windows 98 开始，共享就给许多的上网用户带来无穷无尽的烦恼，成为黑客攻击他人计算机的一把利器。网上有很多关于 IPC 入侵的文章，相信大家一定不陌生。要禁止这些共享，可以打开管理工具→计算机管理→共享文件夹→共享，在相应的共享文件夹上右击，选择停止共享即可。不过机器重新启动后，这些共享又会重新开启。如何彻底禁止 Windows 系统的共享漏洞呢？

（1）查看共享资源

Windows 2000/2003 安装好以后，系统会创建一些隐藏的共享。在 Windows 系统中，计算机所有的驱动器都默认为自动共享，但不会显示共享的手形标志，这就给网络安全留下了隐患。可以在“运行”栏中输入 cmd 然后回车，打开命令提示符，再输入 net share 查看计算机中的共享资源，找到这些共享目录。默认共享目录路径和功能如下所示。

① C＄、D＄、E＄：每个分区的根目录，Windows 2000 pro 版中，只有 Administrator 和 Backup Operators 成员才可连接，Windows 2000 server、Windows server 2003 版本中 Server Operatros 组也可以连接到这些共享目录。

② ADMIN＄ ％SYSTEMROOT％：远程管理用的共享目录。它的路径永远都指向 Windows 2000 的安装路径，比如 c：winnt。

③ FAX＄：在 Windows 2000 Server 中，FAX＄在 fax 客户端发传真的时候会用到。

④ IPC＄：空连接，IPC＄共享提供了登录到系统的能力。

⑤ Net Logon：在 Windows 2000 服务器的 Net Login 服务处理登录域请求时要用到。

⑥ PRINT＄ ％SYSTEMROOT％\SYSTEM32\SPOOL\DRIVERS：用户远程管理打印机。

如果对“命令提示符”的界面不习惯，可以依次打开“控制面板”→“管理工具”→“计算机管理”→“共享文件夹”，查看计算机中所有共享的资源。

(2) 清除共享漏洞

首先确保以 Administrator 或 Power Users 组的成员身份登录系统，然后通过以下三个步骤清除共享的漏洞。

① 选择“开始菜单→控制面板→管理工具→服务”命令，找到 Server 服务，停止该服务，并且在“属性”中将“启动类型”设置为“手动”或“已禁用”。

② 修改注册表。选择“开始→运行”命令，输入 regedit 进入“注册表编辑器”。找到 HEKY_LOCAL_MANCHINE\System\CurrentControlSet\Services\LanmanServer\Paramaters 子键，在右侧的窗口中分别新建一个名为 AutoShareWks 和一个名为 AutoShareServer 的双字节键值，并且将值设置为 0。

③ 使用命令提示符下的 net share 命令也可以消除这一隐患。打开 Windows 自带的记事本，输入如下内容。

```
net share admin$ /del
net share ipc$ /del
net share c /del
```

接下来将该文件保存为一个扩展名为 bat 的批处理文件。最后，用 Windows 的“任务计划”功能让该批处理文件在每次开机时都自动运行。

**提示**：如果还有其他盘也使用了共享，如 D 盘，则在记事本中添加 net share d/del 即可。输入时不要忽略参数之前的空格。

3) 禁止 dump file 的产生

dump 文件在系统崩溃和蓝屏的时候是一份很有用的帮助查找问题的资料。然而，它也能够给黑客提供些敏感信息，比如一些应用程序的密码等。要禁止它，打开“控制面板”→“系统属性”→“高级”→“启动和故障恢复”把“写入调试信息”改成“无”即可。要用的时候，可以重新打开它。

4) 使用文件加密系统 EPS

Windows 2000/2003 强大的加密系统能够给磁盘、文件夹、文件加上一层安全保护。这样可以防止别人把硬盘挂到别的机器上读出里面的数据。记住要给文件夹也使用 EFS，而不仅仅是单个的文件。有关 EFS 的具体信息可以查看 http://www.microsoft.com/windows2000/techinfo/howitworks/security/encrypt.asp。

5) 加密 temp 文件夹

一些应用程序在安装和升级的时候，会把一些东西复制到 temp 文件夹，但是当程序升级完毕或关闭的时候，它们并不会自己清除 temp 文件夹的内容。所以，给 temp 文件夹加密可以给里面的文件多层保护。

6) 锁住注册表

在 Windows 2000/2003 中，只有 Administrators 和 Backup Operators 才有从网络上访问注册表的权限。如果觉得还不够的话，可以进一步设定注册表访问权限，详细信息请参考：

```
http://support.microsoft.com/support/kb/articles/Q153/1/83.asp
```

7）关机时清除掉页面文件

页面文件也就是调度文件，是 Windows 2000/2003 用来存储没有装入内存的程序和数据文件部分的隐藏文件。一些第三方的程序可以把一些没有加密的密码存在内存中，页面文件中也可能会有另外一些敏感的资料。要在关机的时候清除页面文件，可以编辑注册表：

```
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
```

把 ClearPageFileAtShutdown 的值设置成 1。

8）禁止从软盘和 CD ROM 启动系统

一些第三方的工具能通过引导系统来绕过原有的安全机制。如果服务器对安全要求非常高，可以考虑使用可移动软盘和光驱。把机箱锁起来也不失为一个好方法。

9）考虑使用智能卡来代替密码

对于密码，总是让安全管理员进退两难，容易受到 10phtcrack 等工具的攻击。如果密码太复杂，用户为了记住密码，又会把密码到处乱写。如果条件允许，用智能卡来代替复杂的密码是个很好的解决方法。

10）考虑使用 IPSec

正如其名字的含义，IPSec 提供 IP 数据包的安全性。IPSec 提供身份验证、完整性和可选择的机密性。发送方计算机在传输之前加密数据，而接收方计算机在收到数据之后解密数据。利用 IPSec 可以使得系统的安全性能大大增强。

## 4.4 UNIX 系统的安全

UNIX 系统的运行是否安全稳定，与系统管理员对系统的安全配置有着直接的关系。在 UNIX 系统中，系统管理员一般是以超级用户的身份进入系统的，因为 UNIX 的一些系统管理命令只能由超级用户运行。超级用户拥有其他用户所没有的特权，它不管文件存取许可方式如何，都可以读写任何文件，运行任何程序。系统管理员通常使用命令“/bin/su”或以 root 进入系统从而成为超级用户。在后面文章中以 # 表示应输入必须由超级用户运行的命令，用 $ 表不应输入由所有其他用户运行的命令。本节将从系统管理员的角度，讨论 UNIX 系统的安全问题。

### 4.4.1 系统安全管理

安全管理主要分为四个方面。

#### 1. 防止未授权存取

这是计算机安全最重要的问题。要防止未被授权使用系统用户进入系统。用户意识、良好的密码管理（由系统管理员和用户双方配合）、登录活动记录和报告、用户和网络活动的周期检查，这些都是防止未授权存取的关键。

### 2. 防止泄密

这也是计算机安全的一个重要问题。防止已授权或未授权的用户相互存取重要信息。文件系统查账、su 登录和报告、用户意识、加密都是防止泄密的关键。

### 3. 防止用户拒绝系统的管理

这一方面的安全应由操作系统来完成。一个系统不应被一个有意试图使用过多资源的用户损害。不幸的是，UNIX 不能很好地限制用户对资源的使用，一个用户能够使用文件系统的整个磁盘空间，而 UNIX 基本不能阻止用户这样做。系统管理员最好用 PS 命令、记账程序 df 和 du 周期地检查系统，查出过多占用 CUP 的进程和最大占用磁盘的文件。

### 4. 防止丢失系统的完整性

这一安全方面与一个好系统管理员的实际工作(例如，周期地备份文件系统，系统崩溃后运行 fsck 检查修复文件系统，当有新用户时检侧该用户是否可能使用会造成系统崩溃的软件)和保持一个可靠的操作系统有关(即用户不能经常性地使系统崩溃)。

### 5. 运行权限

UNIX 系统要采用单用户方式启动，使系统管理员在允许普通用户登录以前，先检查系统操作，确保系统一切正常。当系统处于单用户方式时，控制台作为超级用户，命令提示符是“♯”。

系统管理员要确切知道/etc/inittab 中的程序做什么工作，确保这些程序以及这些程序所在的目录直到/和/etc/inittb，除 root 外无人可写。

shutdown 只能由作为 root 登录的用户从系统控制台上运行，所以任何的 shutdown 运行的命令只能对 root 可写。

在 UNIX 系统是多用户方式时运行，还要确保/usr/lib/crontab 和该表中列出的任何程序对任何人不可写。如果用户需要由 cron 执行一个程序，系统管理员可用 su 命令在 crontab 表中建立一个入口，使用户的程序不能获得 root 的权限。

每当用户(包括 root 在内)登录时，由 shell 执行/etc/profile 文件，应确保这个文件以及从这个文件运行的程序和命令都只对 root 可写。

## 4.4.2 文件系统安全

### 1. UNIX 文件系统概述

UNIX 文件系统是 UNIX 系统的心脏部分，提供了层次结构的目录和文件。文件系统将磁盘空间划分成一个一个由 1024 个字节组成的块(block)(也有用 512 字节为一块的，如 SCO XENIX)，编号从 0 开始到整个磁盘的最大块数。全部块可划分为四个部分，块 0 称为引导块，文件系统不用该块；块 1 称为专用块，专用块含有许多信息，其中有磁

盘大小和全部块的其他两部分的大小。从块2开始是i节点表,i节点表中含有i节点,表的块数是可变的。

设备文件 UNIX系统与连在本系统上的各种设备之间的通信,通过特别文件来实现。就程序而言,磁盘是文件,MODEM是文件,甚至内存也是文件。所有连接到系统上的设备都在/dev目录中有一个文件与其对应。当在这些文件上执行I/O操作时,由UNIX系统将I/O操作转换成实际设备的动作。例如,文件/dev/mem是系统的内存,如果用cat命令执行这个文件,实际上是在终端显示系统的内存。为了安全起见,这个文件对普通用户是不可读的。因为在任一给定时间,内存区可能含有用户登录密码或运行程序的密码和某部分文件的编辑缓冲区,而缓冲区可能含有用ed - x命令解密后的文本,以及用户不愿让其他人存取的种种信息。在/dev中的文件通常称为设备文件,用ls /dev命令可以看看系统中的一些设备:acuo为呼叫自动拨号据;console为系统控制台;dsknn为块方式操作磁盘分区;kmem为核心内存;mem为内存;lp为打印机;mto为块方式操作磁带;rdsknn为流方式操作的磁盘分区;rmto为流方式操作的磁带;swap为交换区;syscon为系统终端;ttynn为终端口;x25为网络端口等。

**2. 安全考虑**

将设备处理成文件,使得UNIX程序独立于设备,即程序不必一定要了解正在使用的设备的任何特性,存取设备也不需要记录长度、块大小、传输速度、网络协议等这样一些信息。所有的细节由设备驱动程序去关心考虑,要存取设备,程序只须打开设备文件,然后作为普通的UNIX文件来使用。从安全的观点来看这样处理很好,因为任何设备上进行的I/O操作只经过了少量的渠道(即设备文件),用户不能直接地存取设备。所以,如果正确地设置了磁盘分区的存取许可,用户就只能通过UNIX文件系统存取磁盘。文件系统有内部安全机制(文件许可)。不幸的是,如果磁盘分区设置得不正确,任何用户都能够写一个程序读磁盘分区中的每个文件,做法很简单就是读一个i节点,然后以磁盘地址表中块号出现的顺序,依次读这些块号指出的存有文件内容的块。故除了root以外,绝不要使盘分区对任何人可写。因为所有者、文件存取许可方式等这样一些信息存放于i节点中,任何人只要具有已安装分区的写许可,就能设置任何文件的SUID许可,而不管文件的所有者是谁,也不必用chmod(1)命令,还可避过系统建立的安全检查。

以上所述对内存文件mem、kmem和对换文件swap也是一样的。这些文件含有用户信息,一个“别有用心”的程序就可以将用户信息提取出来。要避免磁盘分区(以及其他设备)可读可写,应当在建立设备文件前先用umask命令设置文件建立屏蔽值。一般情况下,UNIX系统上的终端口对任何人都是可写的,从而使用户可以用write命令发送信息。虽然write命令易引起安全方面的问题,但大多数用户觉得用write得到其他用户的信息很方便,所以,系统将终端设备的存取许可设置成对所有用户可写。/dev目录应当采用文件的所有者(属root所有)具有读、写和执行的权利,而同组用户和其他用户只有读和执行权利的存取许可方式。不允许除root外的任何用户读或写盘分区的原则有一例外,即一些程序(通常是数据库系统)要求对磁盘分区直接存取。解决这个问题的经验是盘分区应当由这种程序专用(不安装文件系统),而且应当告知使用这种程序的用

户,文件安全保护将由程序自己而不是 UNIX 文件系统完成。

系统管理员应当做一个程序以定期检查系统中的各个系统文件,包括检查设备文件和 SUID、SGID 程序,尤其要注意检查 SUID、SGID 程序,检查/etc/passwd 和/etc / group 文件,寻找久未登录的户头和校验各重要文件是否被修改。

### 3. 安装和拆卸文件系统

UNIX 文件系统是可安装的,这意味着每个文件系统可以连接到整个目录树的任意节点上(根目录总是被安装上的)。安装文件系统的目录称为安装点。/etc/mount 命令用于安装文件系统,用这条命令可将文件系统安装在现有目录结构的任意处。安装文件系统时,安装点的文件和目录都是不可存取的,因此未安装文件系统时,不要将文件存入安装点目录。文件系统安装后,安装点的存取许可方式和所有者将改变为所安装的文件根目录的许可方式和所有者。安装文件系统时要小心:安装点的属性会改变。还要注意新建的文件,除非新文件系统是由标准文件建立的,系统标准文件会设置适当的存取许可方式,否则新文件系统的存取许可将是对所有用户都具有读、写和执行的权利。可用 -r 选项将文件系统安装成只读文件系统。需要写保护的带驱动器和磁盘应当以这种方式来安装。

不带任何参数的/etc/mount 可获得系统中所安装的文件系统的有关信息。包括文件系统被安装的安装点目录,对应/dev 中的哪个设备,只读或可读写,安装时间和日期等。从安全的观点来讲,可安装系统的危险来自用户可能请求系统管理员为其安装用户自己的文件系统。如果安装了用户的文件系统,则应在允许用户存取文件系统前,先扫描用户的文件系统,搜索 SUID/SGID 程序和设备文件。在除了 root 外任何人不能执行的目录中安装文件系统,用 find 命令或 secure 列出可疑文件,删除不属于用户所有文件的 SUID/SGID 许可。用户文件系统用完后,可用 umount 命令卸下文件系统,并将安装点目录的所有者改回 root 存取许可改为文件的所有者(属 root 所有)具有读、写和执行的权利,而同组用户和其他用户只有读和执行的权利的存取许可方式。

### 4. 系统目录和文件

UNIX 系统中有许多文件不允许用户写,如/bin、/usr/bin、/usr/lbin、/etc/passwd、/usr/lib/crontab、/unix、/etc/rc、/etc/inittab 这样一些文件和目录(大多数的系统目录),可写的目录允许移动文件,会引起安全问题。系统管理员应该经常检查系统文件和目录的许可权限和所有者。可做一个程序,根据系统提供的规则文件(在/etc/permlist 文件中)所描述的文件所有者和许可权规则检查各文件。

**注意:**如果系统的安全管理不好,或系统是新安装的,其安全程序不够高,可以用 make 方式在安全强的系统上运行上述程序,将许可规则文件复制到新系统来,再以设置方式在新系统上运行上述程序,就可提高本系统的安全程序。但要记住,两个系统必须运行相同的 UNIX 系统版本。

### 5. 重要的系统文件

1）/etc/passwd 文件

/etc/passwd 文件是 UNIX 安全的关键文件之一。该文件用于用户登录时校验用户的密码，当然应该仅对 root 可写。文件中每行的一般格式为：

```
LOGNAME:PASSWORD:UID:GID:USERINFO:HOME:SHELL
```

每行的头两项是登录名和加密后的密码，后面的两个数是 UID 和 GID，接着的一项是系统管理员想写入的有关该用户的任何信息，最后两项是两个路径名，一个是分配给用户的 HOME 目录；第二个是用户登录后将执行的 shell(若为空格则默认为/bin/sh)。

（1）密码时效。

/etc/passwd 文件的格式使系统管理员能要求用户定期地改变他们的密码。在密码文件中可以看到，有些加密后的密码有逗号，逗号后有几个字符和一个冒号，例如：

```
steve:xyDfccTrtl80x, M.   y8:0:0:admin:/:/bin/sh
restrict: pom Tkl09Jky4l, 1:0:0:admin:/:/bin/sh
pat:xmotTVoyumjls:0:0:admin:/:/bin/sh
```

可以看到，steve 的密码逗号后有 4 个字符，restrict 有 2 个，pat 没有逗号。逗号后第一个字符是密码有效期的最大周数。第二个字符决定了用户再次修改口信之前，原密码应使用的最小周数(这就防止了用户改了新密码后立刻又改回成旧密码)。其余字符表明密码最新修改时间。要能读懂密码中逗号后的信息，首先必须知道如何用 passwd_esc 计数，计数的方法是：.＝0、/＝1、0-9＝2-11、A-Z＝12-37 、a-z＝38-63。系统管理员必须将前两个字符放进/etc/passwd 文件，以要求用户定期地修改密码，另外两个字符当用户修改密码时，由 passwd 命令填入。

**注意：** 若想让用户修改密码，可在最后一次密码被修改时，放两个“.”，则下一次用户登录时将被要求修改自己的密码。当最大周数(第一个字符)小于最小周数(第二个字符)时，则不允许用户修改密码，仅超级用户可以修改用户的密码。当第一个字符和第二个字符都是“.”时，用户下次登录时被要求修改密码。修改密码后，passwd 命令将“.”删除，此后不会再要求用户修改密码。

（2）UID 和 GID。

/etc/passwd 中 UID 信息很重要，系统使用 UID 而不是登录名区别用户。一般来说，用户的 UID 应当是独一无二的，其他用户不应当有相同的 UID 数值。根据惯例，从 0 到 99 的 UID 保留用作系统用户的 UID(root、bin、uucp 等)。如果在/etc/passwd 文件中两个不同的入口项有相同的 UID，则这两个用户对相互的文件具有相同的存取权限。

2）/etc/group 文件

/etc/group 文件含有关于小组的信息，/etc/passwd 中的每个 GID 在本文件中应有相应的入口项，入口项中列出了小组名和小组中的用户。这样可以方便地了解每个小组的用户，否则必须根据 GID 在/etc/passwd 文件中从头至尾地寻找同组用户。/etc/group 文件对小组的许可权限的控制并不是必要的，因为系统用 UID 和 GID(取自/etc/

passwd)决定文件存取权限,即使/etc/group 文件不存在于系统中,具有相同的 GID 用户也可以小组的存取许可权限共享文件。

小组就像登录用户一样可以有密码。如果/etc/group 文件入口项的第二个域为非空。则将被认为是加密密码,newgrp 命令将要求用户给出密码,然后将密码加密,再与该域的加密密码比较。给小组建立密码一般不是个好做法。首先,如果小组内共享文件,若有某人猜出小组密码,则该组的所有用户的文件就可能泄露。其次,管理小组密码很费事,因为对于小组没有类似的 passwd 命令。可用/usr/lib/makekey 生成一个密码写入/etc/group。

以下情况必须建立新组:可能要增加新用户,该用户不属于任何一个现有的小组;有的用户可能时常需要独自为一个小组;有的用户可能有一个 SGID 程序,需要独自为一个小组;有时可能要安装运行 SGID 的软件系统,该软件系统需要建立一个新组。要增加一个新组,必须编辑该文件,为新组加一个入口项。由于用户登录时,系统从/etc/passwd 文件中取 GID,而不是从/etc/group 中取 GID,所以,group 文件和密码文件应当具有一致性。对于一个用户的小组,UID 和 GID 应当是相同的。多用户小组的 GID 应当不同于任何用户的 UID,一般为 5 位数,这样在查看/etc/passwd 文件时,就可根据 5 位数据的 GID 识别多用户小组,这将减少增加新组及新用户时可能产生的混淆。

## 4.4.3 增加、删除、移走用户

### 1. 增加用户

增加用户有三个过程:首先在/etc/passwd 文件中写入新用户的入口项,然后为新登录用户建立一个 HOME 目录,最后在/etc/group 中为新用户增加一个入口项。在/etc/passwd 文件中写入新的入口项时,密码部分可先设置为 NOLOGIN,以免有人作为此新用户登录。在修改文件前,应 mkdir/etc/ptmp,以免他人同时修改此文件。新用户一般独立为一个新组,GID 号与 UID 号相同(除非他要加入目前已存在的一个组),UID 号必须和其他人不同,HOME 目录一般在/usr 或/home 目录下建立一个以用户登录名为名称的目录作为其主目录。

### 2. 删除用户

删除用户与加用户的工作正好相反,首先在/etc/passwd 和/etc/group 文件中删除用户的入口项,然后删除用户的 HOME 目录和所有文件。用 rm -r /usr/loginname 删除整个目录树。如果用户在/usr/spool/cron/crontabs 中有 crontab 文件,也应当删除。

### 3. 将用户移到另一个系统

这是一个复杂的问题,不只是复制用户的文件和用户在/etc/passwd 文件中的入口项。首先一个问题是用户的 UID 和 GID 可能已经用于另一个系统,若是出现这种情况,必须给要转移的用户分配另外的 UID 和 GID。如果改变了用户的 UID 和 GID,则必须搜索该用户的全部文件,将文件的原 UID 和 GID 改成新的 UID 和 GID。用 find 命令可

以完成这一修改。

```
find -user olduid -exec chown newuid {}
find -group oldgid -exec chgrp newgid {}
```

也许还要为用户移走其他一些文件,如/usr/mail/user 和/usr/spool/cron/crontabs/user。如果用户从一个不是本系统管理员的系统移来,则应对该用户的目录结构运行程序来检查。一个不安全系统的用户,可能有与该用户其他文件存在一起的 SUIU/SGID 程序,而这个 SUID/SGID 程序属于另一个用户。在这种情况下,如果用 cpio 或 tar 命令将用户的目录结构复制到本系统,SUID/SGID 程序也将会复制到本系统而没有任何警告信息。应当在允许用户使用新系统以前先删除这种文件的 SUID/SGID 许可。总之,始终坚持检查所移用户的文件总是更安全些。也可以用 su 命令进入用户的户头,再复制用户文件,这样文件的所有者就是该用户,而不是 root。

### 4.4.4 安全检查

像 find 和 secure 这样的程序称为检查程序,它们搜索文件系统,寻找出 SUID/SGID 文件、设备文件、任何人可写的系统文件、设有密码的登录用户、具有相同 UID/GID 的用户等。

**1. 记账**

UNIX 记账软件包可用作安全检查工具,除最后登录时间的记录外,记账系统还能保存全天运行的所有进程的完整记录。对于一个进程所存储的信息包括 UID、命令名、进程开始执行与结束的时间、CPU 时间和实际消耗的时间、该进程是否是 root 进程等,这将有助于系统管理员了解系统中的用户在干什么。acctcom 命令可以列出一天的账目表。有时,系统中有多个记账数据文件,记账信息保存在文件/usr/adm/pacct * 中,/usr/adm/pacct 是当前记录文件,/usr/adm/pacctn 是以前的记账文件(n 为整型数)。若有若干个记账文件要查看,可在 acctcom 命令中指定文件名:acctcom/usr/adm/pacct?。/usr/adm/paect 要检查问题的其中之一是在 acctcom 的输出中查找一个用户过多的登录过程,若有,则说明可能有人一遍遍地尝试登录,猜测密码,企图非法进入系统。此外,还应查看 root 进程,除了系统管理员用 su 命令从终端进入 root、系统启动、系统停止时间以及由 init(通常 init 只启动 getty、login、登录 shell)、cron 启动的进程和具有 root SUID 许可的命令外,不应当有任何 root 进程。由记账系统也可获得有关每个用户的 CPU 利用率、运行的进程数等统计数据。

**2. 其他检查命令**

du:报告在层次目录结构(当前工作目录或指定目录起)中各目录占用的磁盘块数,可用于检查用户对文件系统的使用情况。

df:报告整个文件系统当前的空间使用情况。可用于合理调整磁盘空间的使用和管理。

ps：检查当前系统中正在运行的所有进程。对于用了大量 CPU 时间的进程、同时运行了许多进程的用户及运行了很长时间但用了很少 CPU 时间的用户进程应当深入检查。还可以查出运行了一个无限制循环的后台进程的用户和未注销户头就关终端的用户(一般发生在直接连线的终端)。

who：可以告诉系统管理员系统中工作的进展情况等信息，检查用户的登录时间和登录终端。

su：每当用户试图使用 SU 命令进入系统用户时，命令将在/usr/adm/sulog 文件中写一条信息。若该文件记录了大量试图用 su 进入 root 的无效操作信息，则表明了可能有人企图破译 root 密码。

login：在一些系统中，login 程序记录了无效的登录企图。若本系统的 login 程序不做这项工作而系统中有 login 源程序，则应修改 login。每天总有少量的无效登录，若无效登录的次数突然增加了两倍，则表明可能有人企图通过猜测登录名和密码，非法进入系统。

最重要的是系统管理员越熟悉自己的用户和用户的工作习惯，就越能快速发现系统中任何不寻常的事件，而不寻常的事件意味着系统已被人窃密。

### 3. 安全检查程序的问题

若有诱骗，则这些方法中没有几个能防诱骗。如 find 命令，如果碰到路径名长于 256 个字符的文件或含有多于 200 个文件的目录，将放弃处理该文件或目录，用户就有可能利用建立多层目录结构或大目录隐藏 SUID 程序，使其逃避检查。但 find 命令会给出一个错误信息，系统管理员应手工检查这些目录和文件。也可用 ncheck 命令搜索文件系统，但它没有 find 命令指定搜索哪种文件的功能。如果定期存取 profile 文件，则检查久未登录用户的方法就不奏效了。而用户用 su 命令时，除非用参数“-”，否则 su 不读用户的 profile。

有三种方法可寻找久未登录的账户。

UNIX 记账系统在文件/usr/adm/acct/sum/login 中为每个用户保留了最后一次登录日期。用这个文件的好处是该文件由系统维护，所以可完全肯定登录日期是准确的。缺点是必须在系统上运行记账程序以更新 loginlog 文件，如果在清晨(午夜后)运行记账程序，一天的登录日期可能就被清除了。

/etc/passwd 文件中的密码时效域将能告诉系统管理员，用户的密码是否过期了。若过期，则意味着自过期以来，户头再未被用过。这一方法的好处在于系统记录了久未用的户头，检查过程简单，且不需要记账系统所需要的磁盘资源。缺点是也许系统管理员不想在系统上设置密码时效，而且这一方法仅在密码的最大有效期(只有几周)才是准确的。

系统管理员可以写一个程序，每天和重新引导系统时扫描/etc/wtmp，自己保留下用户最后登录时间记录。这一方法的好处是不需要记账程序，并且时间准确，缺点是要自己写程序。

以上任何方法都可和/usr/adm/sulog 文件结合起来，查出由 login 或 su 登录户头的

最后登录时间。如果有人存心破坏系统安全，第一件要做的事就是寻找检查程序。破坏者将修改检查程序，使其不能报告任何异常事件，也可能停止系统记账，删除记账文件，使系统管理员不能发现破坏者干了些什么。

#### 4. 系统泄密后怎么办？

发现有人已经破坏了系统安全的时候，系统管理员首先应做的是面对肇事用户。如果该用户所做的事不是蓄意的，而且公司没有关于“破坏安全”的规章，也未造成损坏，则系统管理员只需清理系统，并留心该用户一段时间。如果该用户造成了某些损坏，则应当报告有关人士，并且应尽可能地将系统恢复到原来的状态。如果肇事者是非授权用户，那就表明肇事者已设法成为 root 且本系统的文件和程序已经泄密了。

系统管理员应当想法查出谁是肇事者，他造成了什么损坏？还应当对整个文件做一次全面的检查，并不只是检查 SUID 和 SGID 及设备文件。如果系统安全被一个敌对的用户破坏了，应当采用下面的步骤。

(1) 关系统，然后重新引导，不要进入多用户方式，进入单用户方式。安装含有本系统原始 UNIX 版本的磁带和软盘。将/bin、/usr/bin、/etc、/usr/lib 中的文件复制到一个暂存目录中，将暂存目录中所有文件的校验和(用原始版本的 sum 程序复制作校验和，不要用/bin 中的 sum 程序作)与系统中所有对应的文件的校验和进行比较，如果有任何差别，要查清差别产生的原因。如果两个校验和不同，是由于安装了新版本的程序，确认一下是否的确是安装了新版本程序。如果不能找出校验和不同的原因，用暂存目录中的命令替换系统中的原有命令。在确认系统中的命令还未被篡改之前，不要用系统中原命令。用暂存目录中的 shell，并将 PATH 设置为仅在暂存目录中搜索命令。根据暂存目录中所有系统命令的存取许可，检查系统中所有命令的存取许可和所有系统目录的存取许可。如果用了 perms，检查 permlist 文件是否被篡改过。如果系统 UNIX(/unix)的校验和不同于原版的校验和，并且系统管理员从未修改过内核，则应当认为非法者“很能干”，从暂存缓冲区重新装入系统。系统管理员可以从逐步增加的文件系统备份中恢复用户的文件，但是在检查备份中的“有趣”文件之前，不能做文件恢复。

(2) 改变系统中的所有密码，通知用户他们的密码已改，应找系统管理员得到新密码。

(3) 当用户来要新密码时，告诉用户发生了一次安全事故，他们应查看自己的文件和目录是否潜伏着危害(如 SUID 文件、特洛伊木马、任何人可写的目录)，并报告系统管理员任何异乎寻常的情况。

(4) 设法查清安全破坏是如何发生的。如果没有肇事者，说明这也许是不可能弄清的。如果能发现肇事者如何进入系统，设法堵住这个安全漏洞。第一次安装 UNIX 系统时，可以将 shell、sum 命令，所有文件的校验和存放在安全的介质上(磁带、软盘、硬盘和任何可以卸下并锁起来的介质)。于是不必再从原版系统磁带上重新装入文件，可以安装备份介质，装入 shell 和 sum，将存在磁带上的校验和与系统中文件的校验和进行比较。系统管理员也可以自己写一个计算校验和的程序，破坏者将不能知道该程序的算法。如果将该程序及校验和保存在磁带上，这一方法的保密问题就减小到一个物理的安

全问题，即只需将磁带锁起来。

## 4.4.5 安全意识

### 1. 用户安全意识

UNIX 系统管理员的职责之一是保证用户安全，这其中一部分工作是由用户的管理部门来完成。但是作为系统管理员，有责任发现和报告系统的安全问题，因为系统管理员负责系统的运行。

避免系统安全事故的方法是预防性的，当用户登录时，其 shell 在给出提示前先执行/etc/profile 文件，要确保该文件中的 PATH 指定最后搜索当前工作目录，这样将减少用户能运行特洛伊木马的机会。将文件建立屏蔽值的设置放在该文件中也是很合适的，可将其值设置成至少要防止用户无意中建立任何人都能写的文件。要小心选择此值，如果限制太严，则用户会在自己的 profile 中重新调用 umask 以抵制系统管理员的意愿，如果用户大量使用小组权限共享文件，系统管理员就要设置限制小组存取权限的屏蔽值。系统管理员必须建立系统安全和用户的"痛苦量"间的平衡(痛苦量是安全限制引起的愤怒的函数)。

定期地用 grep 命令查看用户 profile 文件中的 umask，可了解系统安全限制是否超过了用户痛苦极限。系统管理员可每星期随机抽选一个用户，将该用户的安全检查结果(用户的登录情况简报和 SUID/SGID 文件列表等)发送给他的管理部门和他本人。主要有四个目的：大多数用户会收到至少有一个文件检查情况的邮件，这将引起用户考虑安全问题(虽然并不意味着用户们会采取加强安全的行动)；有大量可写文件的用户，将一星期得到一次邮件，直到他们取消可写文件的写许可为止。冗长的烦人的邮件信息也许足以促使这些用户采取措施，删除文件的写许可；邮件将列出用户的 SUID 程序，引起用户注意自己有 SUID 程序，使用户知道是否有不是自己建立的 SUID 程序；送安全检查表可供用户管理自己的文件，并使用户知道对文件的管理关系到数据安全。如果系统管理员打算这样做，应事先让用户知道，以便他们了解安全检查邮件的目的。发送邮件是让用户具有安全意识，不要抱怨发送邮件。

管理意识是提高安全性的另一个重要因素。如果用户的管理部门对安全要求不强烈，系统管理员可能也忘记强化安全规则。最好让管理部门建立一套每个人都必须遵守的安全标准，如果系统管理员在此基础上再建立自己的安全规则，就强化了安全。管理有助于加强用户意识，让用户明确，信息是有价值的资产。

系统管理员应当使安全保护方法对用户尽可能地简单，提供一些提高安全的工具，如公布锁终端的 lock 程序，让用户自己运行 secure 程序；将 pwexp(检查用户密码信息的程序)放入/etc/profile 中，使用户知道自己的密码时间。多教给用户一些关于系统安全的知识，确保用户知道自己的许可权限和 umask 命令的设置值。如果注意到用户在做蠢事时，就给他们一些应当怎样做才对的提示。用户知道的关于安全的知识越多，系统管理员在保护用户利益方面做的事就越少。

### 2. 保持系统管理员个人的登录安全

若系统管理员的登录密码泄密了，则窃密者离窃取 root 只有一步之遥了。因为系统管理员经常作为 root 运行，窃密者非法进入到系统管理员的户头后，将用特洛伊木马替换系统管理员的某些程序，系统管理员会作为 root 运行这些已被替换的程序。正是因为这个原因，在 UNIX 系统中，管理员的账户最常受到攻击。即使 su 命令通常要在任何都不可读的文件中记录所有想成为 root 的企图，还可用记账数据或 ps 命令识别运行 su 命令的用户。也正是如此，系统管理员作为 root 运行程序时应当特别小心，因为最微小的疏忽也可能“沉船”。下列一些指导规则可使系统管理员驾驶一艘“坚固的船”。

(1) 不要作为 root 或以自己的登录账户运行其他用户的程序，首先用 su 命令进入用户的账户。

(2) 绝不要把当前工作目录排在 PATH 路径表的前边，那样实际是在招引特洛伊木马。当系统管理员用 su 命令进入 root 时，他的 PATH 将会改变，就让 PATH 保持这样，以避免特洛伊木马的侵入。输入/bin/su 执行 su 命令。若有 su 源码，将其改成必须用全路径名运行，即 su 要确认 argv[0]的头一个字符是“/”才运行。随着时间的推移，用户和管理员将养成输入/bin/su 的习惯。不要未注销户头就离开终端，特别是作为 root 用户时更不能这样。当系统管理员作为 root 用户时，命令提示符是“#”，这个提示符对某些人来说可能是个红灯标志。

(3) 不允许 root 在除控制台外的任何终端登录(这是 login 的编译时的选项)。如果没有 login 源码，就将登录名 root 改成别的名，使破坏者不能在 root 登录名下猜测各种可能的密码，从而非法进入 root 的户头。还要经常改变 root 的密码。确认 su 命令记下的想运行 su 企图的记录/usr/adm/sulog，该记录文件的许可方式是 600，并属 root 所有。这是非法者喜欢选择来替换成特洛伊木马的文件。不要让某人作为 root 运行，即使是几分钟或是系统管理员在一旁注视着也不行。

### 3. 保持系统安全

要考虑系统中一些关键的薄弱环节：系统是否有 MODEM? 电话号码是否公布? 系统是否连接到? 还有什么系统也连接到该网络? 系统管理员是否使用未知来处或来处不可靠的程序? 系统管理员是否将重要信息放在系统中? 系统的用户是熟悉系统的使用还是新手? 用户是否很重视关心安全? 用户的管理部门是否重视安全?

保持系统文件安全的完整性。检查所有系统文件的存取许可，任何具有 SUID 许可的程序都是非法者想偷换的选择对象。要特别注意设备文件的存取许可。要审查用户目录中具有系统 ID/系统小组的 SUID/SGID 许可的文件。在未检查用户的文件系统的 SUID/SGID 程序和设备文件之前，不要安装用户的文件系统。将磁盘的备份存放在安全的地方。设置密码时效，如果能存取 UNIX 的源码，将加密密码和信息移到仅对 root 可读的文件中，并修改系统的密码处理子程序，这样可增加密码的安全。修改 passwd，使 passwd 能删去密码打头和末尾的数字，然后根据 spell 词典和/etc/passwd 中用户的个人信息，检查用户的新密码，也检查用户新密码中子串等于登录名的情况。如果新密码

是 spell 词典中的单词，或/etc/passwd 中的入口项的某项值，或是登录名的子串，passwd 将不允许用户改变密码。记录本系统的用户及其授权使用的系统。查出久未使用的登录户头，并取消该户头。确保没有无密码的登录户头。启动记账系统。查出不寻常的系统使用情况，如大量的占用磁盘、大量的使用 CPU 时间、大量的进程、大量的使用 su 的企图、大量无效的登录、大量的到某一系统的网络传输及奇怪的 uucd 请求等。修改 shell，使其等待了一定时间而无任务时终止运行。修改 login，使其打印出用户登录的最后时间，三次无效登录后，将通信线挂起，以便系统管理员能检查出是否有人试图非法进入系统。确保 login 不让 root 在除控制台外的任何地方登录。修改 su，使得只有 root 能以过期密码通过 su 进入某一户头。当安装来源不可靠的软件时，要检查源码和 makefile 文件，查看特殊的子程序调用或命令。即使是安装来源可靠的软件，也要检查是否有 SUID(SGID)程序，确认这些许可的确是必要的。如果可能，不要让这些程序具有系统 ID(或组)的 SUID(SGID)许可，而应该建立一个新用户(或给)供该软件运行。

如果系统在办公室中，将 secure、perms 和任何其他做安全检查的 shell 程序存取许可设为仅执行，更好的是将这些 shell 程序存于可移动的介质上。

**注意**：只要系统有任何人都可调用的拨号线，系统就不可能真正的安全。系统管理员可以很好地防止系统受到偶然的破坏。但是那些有耐心、有计划、知道自己在干什么的破坏者，对系统直接的有预谋的攻击却常常能成功。如果系统管理员认为系统已经泄密，则应当设法查出肇事者。若肇事者是本系统的用户，与用户的管理部门联系，并检查该用户的文件，查找任何可疑的文件，然后对该用户的登录小心地监督几个星期。如果肇事者不是本系统的用户，可让本公司采取合法的措施，并要求所有的用户改变密码，让用户知道出了安全事故。让用户们检查自己的文件是否有被篡改的迹象。如果系统管理员认为系统软件已被更改了，就应当从原版系统(或光盘)上重装入所有系统软件，保持系统安全比道歉更好。

### 4.4.6 UNIX 服务裁减

#### 1. inetd

编辑/etc/inetd.conf 文件，注释掉所有不需要的服务(在注释行开始加入“#”)。

其中可以被注释的一些比较有代表性的服务有：shell、login、exec、talk、combat、uucp、tftp、finger、netstat、ruserd、sprayd、walld、rstatd、cmsd、ttdbserverd 等，可以仅保留需要使用的 telnet、FTP、DNS(in.named)等。需要特别注意 solaris 系统自身携带的 DNS(in.named)、FTP、POP、IMAP 等主要服务均有问题。

注释掉服务后可以运行下列命令将 inetd 服务重启。

```
ps -ef | grep inetd
```

使用命令获取 inetd 服务的进程号 pid。

```
kill -9 pid
```

使用命令杀死 inetd 进程。

/usr/sbin/inetd -s

使用命令启动 inetd 服务。

下面列出常用 solaris 版本的 inetd. conf 文件的解释。

```
SunOS 5.5:
name  dgram  udp  wait  root  /usr/sbin/in.tnamed  in.tnamed
```

实现 DARPA 名字服务协议的服务器程序,一般可以被注释。

```
ftp  stream  tcp  nowait  root  /usr/sbin/in.ftpd  in.ftpd
```

实现文件传输协议的服务器程序,一般保留,除非服务器不提供 ftp 服务。

```
telnet  streamt  tcp  nowait  root  /usr/sbin/in.telnetd  in.telnetd
```

实现 telnet 协议的服务器程序,一般保留,除非服务器不提供远程登录服务。

```
shell  stream  tcp  nowait root  /usr/sbin/in.rshd  in.rshd
```

远程 shell 服务,一般可以被注释(远程登录服务,上一项 telnet 即可以实现)。

```
login  stream tep    nowait root  /usr/sbin/in.rloglnd  in.rlogind
```

远程注册服务,一般保留,除非服务器不提供远程登录服务。

```
exec  stream tcp  nowait root  /usr/sbin/in.rexecd  in.rexecd
```

远程执行服务,一般保留,除非服务器不提供远程登录服务。

```
comsat  dgram  udp  wait  root  /usr/sbin/in.comsat  in.comsat
```

监听邮件到来,提醒用户收邮件的服务,一般可以被注释。

```
talk  dgram  udp  wait  root  /usr/sbin/in.talkd  in.talkd
```

提供 talk 服务,一般可以被注释。

```
uucp  stream tcp  nowait root  /usr/sbin/in.uucpd  in.uucpd
```

实现 UINX 到 UNIX 的文件复制,已经被 ftp 所代替,一般可以被注释。

```
Pboot  dgram  udp  wait  root  /usr/sbin/in.tftpd  in.tftpd - s /tft
```

实现内部文件传输服务,一般可以被注释(系统默认值为不启动)。

```
finger  stream  tcp  nowait  nobody  /usr/sbin/in.fingerd  in.fingerd
```

提供显示本地和远程用户的服务,一般可以被注释。

```
systat  stream tcp  nowait root  /usr/bin/ps ps -ef
```

向远端显示本地运行的进程,一般可以被注释。

```
netstat  stream tcp  nowait  root  /usr/bin/netstat  netstat - f inet
```

向远端显示本地网络状态,一般可以被注释。

```
time    stream  tcp  nowait  root  internal
time    dgram   udp  wait    root  internal
```

用作时钟同步,一般可以被注释。

```
echo    stream  tcp  nowait root  internal
echo    dgram   udp  wait   root  internal
discard  stream  tcp  nowait  root  internal
discard  dgram   udp  wait    root  internal
daytime  stream  tcp  nowait root  internal
daytime  dgram   udp  wait   root  internal
chargen  stream tcp  nowait  root  internal
chargen  dgram  udp    wait  root  internal
```

上述这些服务都是测试的时候使用,一般均可以被注释。

```
100232/10  tli  rpc/udp  wait  root  /usr/sbin/sadmind  sadmind
```

分布式系统管理守护进程,存在漏洞较多,应尽量不启动这个服务。

```
rquotad/1  tli  rpc/datagram_v  wait  root  /usr/lib/nfs/rquotad  rquotad
```

远程定额服务,一般可以被注释。

```
rusersd/2-3 tli rpc/datagram_v,circuit_v wait root /usr/lib/nets c/rusers/rpc.rusersd rpc.rusersd
```

网络用户名服务,提供用户名列表,一般可以被注释。

```
sprayd/1  tli  rpc/datagram_v  wait  root  /usr/lib/netsvc/spray/rpc.spra yd  rpc.sprayd
```

提供记录 spray 收发包的记录,一般可以被注释。

```
rpc.rwalld  rpc.rwalldi  rpc/datagram_v  wait  root  /usr/lib/netsvc/rwall/
```

处理 rwall 请求,一般可以被注释。

```
rstatd/2-4  tli  rpc/datagram_v  wait  root  /usr/lib/netsvc/rstat/rpc.rstatd  rpc.rstatd
```

显示内核状态,是一个 rpc 服务,在安全要求较高的情况下应被注释。

```
rexd/1  tli  rpc/tcp  wait  root  /usr/sbin/rpc.rexd  rpc.rexd
```

基于 rpc 的远程执行服务,在安全要求较高的情况下应被注释。

```
00060/2-4  dgram  rpc/udp  wait  root  /usr/openwin/bin/rpc.cmsd  rpc.cmsd
Sun ToolTalk Database Serverp  wait  root  /usr/openwin/bin/rpc.cmsd  rpc.cmsd
```

日历管理服务,rpc 服务,一般可以被注释。

```
rverd83/1  stream  rpc/tcp  wait  root  /usr/dt/bin/rpc.ttdbserverd  rpc.ttdbserverd
```

基于 rpc 的 ToolTalk 数据库服务,一般可以被注释。

```
ver0221/1  tli  rpc/tcp  wait  root  /usr/openwin/bin/kcms  server kcms_server
```

KCMS 库服务守护进程,一般可以被注释。

```
fs  stream  tcp  wait  nobody  /usr/openwin/lib/fs.auto  fs
```

X 字体服务,一般可以被注释,除非启动了 X Window 服务。

```
netbios-ns  dgram  udp  wait  root  /usr/local/samba/nmbd nmbd
```

一般可以被注释。

```
pop3 stream tcp  nowait  root  /export/netmgr/qpopper2.2/popper solaris2popper solaris2
```

一般可以被注释,除非系统作为 mail 服务器,务必及时更新 POP3 的版本。

SunOS 5.6 版本与 SunOS 基本相同,inet.conf 文件中多以下条目。

```
ufsd/1  tli  rpc/*  wait  root  /usr/lib/fs/ufs/ufsd  ufsd-p
```

UFS-aware 服务守护进程,一般可以被注释。

```
100235/1  tli  rpc/tcp  wait  root  /usr/lib/fs/cachefs/cachefsd cachefsd
```

CacheFS 守护进程,一般可以被注释。

```
kerbd/4  tli  rpc/ticlts  wait  root  /usr/sbin/kerbd kerbd
```

与 rpc 服务相关,在安全要求较高的情况下,一般应该被注释。

```
printer  stream  tcp  nowait  root  /usr/lib/print/in.lpd  in.lpd
```

打印机守护进程,一般可以被注释,除非使用打印机。

```
daudio  stream  tcp  wait root  /usr/openwin/bin/Xaserver Xaserver -noauth -inet
```

一般可以被注释。

SunOS 5.7 与上述两版本基本相同。在上述服务中,在只保留必须的服务,并且务必保证运行服务的版本及时更新。

### 2. RC

通过注释掉不必要的 rc 程序,可以使某些服务不启动。对于 Solaris 系统而言,可以在非 MAIL 服务器上注释掉 Sendmail 服务,此外可以在不需要使用 NFS 的环境下注释掉 statd 服务和 automountd 服务。

要注释服务,首先要找它。进入/etc 目录,在 rc0.d 到 rc6.d 的各个目录中,利用 grep 命令搜索自己关心的服务。例如,对于 Sendmail 可以使用“grep sendmail *”命令。发现启动的文件后,把该文件移走即可。

为了防止将来需要使用该文件,建议在/etc 目录下建立 rcbackuprc 目录,把被移动的文件,根据其位置对应存放在 rc0.d 到 rc6.d 的目录中。

大部分服务均可以移走,建议保留的配置文件(各版本基本相同)如下。

Rc0.d:

K00ANNOUNCE  K33audit  K43inet  K35volmgt  K36sendmail(如已安装其他功能类似软件,或非 Mail 服务器则删除)  K40cron(无定时需求则删除)  K83devfsadm  K40nscd(不使用 DNS 则删除)  K41rpc(如不起 X Windows 建议删除)  K37power  K40syslog  K42inetsvc

```
re1.d:
K00ANNOUNCE  K33audit   S0IMOUNTFSYS   K35volmgt   K36sendmail   K36utmpd K40nscd     K37power
K40syslog  K431net
rc2.d:
S69inet    S74syslog    S85power    S88sendmail    S71sysid sys    README    S75savecore  S92volmgt
S01MOUNTFSYS    S72inetsvc    S76nscd    S73cachefs. daemon  S80PRESERVE    S99audit    S20sysetup
S30sysid.net
rc3.d不保留
rc5.d:
S33keymap sh    K40syslog  S40standardmounts sh    K33audit    S42coreadm    K35volmgt  S50devfsadm
K42inetsvc   S50drvconfig   K43inet   S60devlinks   K37power   README   S10initpcmcia   S70buildmnttab.s
  S30rootusr.sh
```

### 4.4.7 Solaris安全配置与管理

Solaris是一款多用户多任务的Unix操作系统，1993年由SunOS改编而来。Solaris系统内核基于AT&T发布的SVR4(即System Ⅴ Release 4)，但Solaris同时也具备了一些BSD版本Unix的特色，目前Solaris的最新版是Solaris 10。Solaris是高科技研究和教育领域使用最多的Unix操作系统之一，目前主要运行在SPARC、x86等硬件平台之上。作为行业领先的UNIX平台，它集成了强大的全新功能，性能、可用性和安全性极高。在默认情况下就能达到B1级别的安全性。

在可靠的Solaris下默认定义了四个角色用于系统管理。

(1) 安全管理员：管理系统中与安全性相关的所有方面，比如审核、登录和密码管理。

(2) 系统管理员：完成所有与安全性无关的系统管理任务，不包括安装新软件。

(3) Root账户：用于安装新软件。

(4) 开放账户：用于进行备份及其他。

必要时需要在系统中增加新的角色来完成其他任务，如数据库管理、Web管理等。在使用Solaris的时候，还需要对以下几个方面的安全问题加以关注。

(1) 本地安全增强：主要任务是限制某些强大命令的访问，设置正确的文件权限，应用组和用户的概念，并使suid/sgid和rw-rw-rw的文件最少。

(2) 网络安全增强：包括使用安全的协议来管理，禁止所有不需要的服务，禁止系统间的信任关系，禁止不需要的账号，增强认证需要的密码，保护存在危险的网络服务，限制访问等。

(3) 应用安全增强：主要包括限制用户的权限，限制进程所有者的权限，检查应用相关文件权限，限制访问其他系统资源，使应用所依赖的suid/sgid文件最少，并使用应用本身的安全特性，以及删除samples和其他无用的组件。

(4) 监控与警报：主要包括日志、完整性、入侵检测等一些使用工具等。

#### 1. 系统配置与参数配置

和所有的操作系统一样，Solaris系统也需要在安装时就要确定安全目标，安装最小

的系统，根据需要增加应用软件。首先需要加强 eeprom 安全，运行“eeprom security=command”系统将改变安全级别，并提示输入密码。对于一般用户，从硬盘启动，不需要输入密码。如果选择从光盘启动，则需要密码。此项为可选配置，视具体需求而定。由于入侵者进入系统后，大部分是利用缓冲溢出取得 root shell 的，为了防止基于堆栈的缓冲区溢出，需要在/etc/system 文件中加入下面内容。

```
set  noexec_user_stack= 1              ;防止在堆栈中执行
set  noexec_user_stack_log= 1          ;当某人试图运行增加一个记录
```

同时需要修改 system 文件的属性，将其设为 644。为了防止电源系统的管理，最好只允许 root 进行电源管理，编辑/etc/default/sys-suspend 文件，将“PERMS=console-owner”修改为“PERMS=.”。为了防止启动后，按 stopfa 或 L1fa 组合键得到 ok 提示符，使用启动盘可以进入单用户模式，防止黑客物理接触机器，需要在/etc/default/kbd 中，改变或加入“KEYBOARD_ABORT=disable”。

### 2. 用户管理

用户管理是系统安全管理上的重要内容，Solaris 除需要遵循上面讲的用户管理的内容外，还需要禁止所有不需要的系统账户。编辑/etc/passwd，将需要禁止账户的 ** 用 NP 代替。需要禁止的账户一般有 bin、daemon、adm、lp、smtp、sys、uucp、nobody、noaccess 等。同时让用户使用强密码，在/etc/default/passwd 中根据需要进行如下设置。

```
PWMIN=1     #最短改变时间
PWMAX=13    #密码最长有效时间
PWWARN=4    #密码失效前几天通知用户
PWLEN=8     #最短密码长度
```

对于用户的登录的安全防范，主要需要修改系统中/etc/default/login 文件，主要包括以下几个内容。

```
SYSLOG= YES        ;需要记录所有 root 登录尝试，以便及时发现入侵企图
TIMEOUT= 120       ;设置 session 超时时间
UMASK= 022         ;设置默认 umask
PASSREQ= YES       ;确保用户登录时提示输入密码
ALTSHELL= YES      ;设置 Shell 环境变量
```

### 3. 系统服务配置

保障网络安全重要一步是通过禁止特定的 IP 端口来阻止非授权的入口，禁用所有不需要的服务，这些服务一般在/etc/service 中启用，并在/etc/inetd.conf 中配置。管理员可以关闭如 name、shell、login、exec、comsat、talk、rusersd、printer、finger、uucp 以及所有以 r 开头的服务。对于那些必须提供的服务，则通过采用 tcpwapper 来保护，并根据需要定义限制的地址。检查 hosts.allow 和 hosts.deny 文件，使用 xinetd 替代 inetd。在系

统启动时，需要禁止所有不需要的服务，在 rc. x 目录中将不需要的服务改名。

```
mv /etc/rc3.d/S92volmgt /etc/rc3.d/KS92volmgt
```

以下服务应该根据需要进行禁止，snmpdx、autofs(Automounter)、volmgt(Volume Deamon)、lpsched(LP print service)、nscd(Name Service Cache Daemon)、Sendmail、keyserv 等。在最新的 Solaris10 中，这些服务可以采取 svcadm 来对应用服务进行管理。如想关闭 smtp 服务，用户可以采用如下命令。

```
#svcadm disable network/smtp: sendmail
```

检查所有的. rhosts 文件，. rhosts 允许不要密码远程访问，预先生成？ $HOME/. rhosts 文件，并且设置为 0000，防止被写入“＋＋”。攻击者经常使用类似符号链接或者利用 ROOTSHELL 写入。

### 4. 网络接口调整和优化

管理员需要在/etc/rc2. d/下的相关文件中做如下参数调整。

```
#ndd-set /dev/arp arp_cleanup_interval 60000          /* 缩短 ARP的 cache保存时间 * /
#ndd-set /dev/ip ip_ire_flush_interval 60000          /* 缩短 ARP表中特定条目的保持时间 * /
#ndd-set /dev/ip ip_respond_to_echo_broadcast 0 /* 关闭 echo广播，防止 ping攻击 * /
#ndd-set /dev/ip ip_forward_src_routed 0              /* 关闭原路由寻址 * /
#ndd-set /dev/ip ip_forwarding 0                      /* 禁止系统转发 IP包 * /
#ndd-set /dev/ip ip_forward_directed_broadcasts 0     /* 禁止系统转发定向广播包 * /
#ndd-set /dev/ip ip_ignore_redirect 1                 /* 使系统忽略重定向 IP包 * /
#ndd-set /dev/ip ip_strict_dst_multihoming 1          /* 使系统限制多宿主机 * /
#ndd-set /dev/ip ip_respond_to_address_mask_broadcast= 0
                                                      /* 确保系统关闭 ICMP广播响应 * /
#ndd-set /dev/ip ip_ip_respond_to_timestamp= 0
                                                      /* 关闭系统对 ICMP时戳请求的响应 * /
#ndd-set /dev/ip ip_ip_respond_to_timestamp_broadcast= 0
                                                      /* 关闭 ICMP时戳广播的响应 * /
#ndd-set /dev/ip ip_send_redirects= 0                 /* 禁止系统发送 ICMP重定向包 * /
```

同时改变 TCP 序列号产生参数，在/etc/default/inetinit 中改变 TCP_STRONG_ISS=2。由于动态路由可能会收到错误的路由信息，所以，建议使用静态路由设置 in. routed 运行在静态路由模式，管理员需要创建/usr/sbin/in. routed 文件，并将这个文件的属性修改为 0755，具体内容如下。

```
#! /bin/sh
/usr/sbin/in.routed.orig - q
```

### 5. 其他安全技术

Solairs 系统的文件管理与 Linux 系统类似，主要也是注意有关 suid 的文件，需要删除所有不使用的 suid 文件，最好删除/etc 下所有组中的可写文件，或者去掉写权限。还

需要确保每个 root 启动的脚本属于 root，改变/var/cron 权限，将其设为 700。开放日志和监控，修改/etc/cron. d/logchecker 中 LIMIT＝4096，这样就将 cron logfiles 的大小设为 2M，并编辑/etc/init. d/inetsvc，需要记录所有 inetd 服务，保证有如下条目。

```
/usr/sbin/ifconfig - au netmask + broadcast + /usr/sbin/inetd -s - t
```

编辑修改 syslog. conf 文件，需要增加下面记录，用来记录 debug 信息。

```
* .debug /var/adm/compass.messages
auth.info /var/log/authlog
```

并创建/var/adm/loginlog 来记录登录失败信息，具体过程如下。

```
#ouch /var/adm/loginlog
#chmod 600 /var/adm/loginlog
#chown root /var/adm/loginlog
#chgrp sys /var/adm/loginlog
```

在系统安装完后，需要安装最新的补丁。安装补丁对系统稳定和安全十分重要，查看更新更安全的补丁在 http://sunsolve. sun. com，用户可以登录使用下面的命令查看系统中安装了那些补丁。

```
#showrev - p
```

任何一种单一的安全措施，防范能力都是有限的，一个安全的系统必须采取多种安全措施，多管齐下才能更好地保证安全。假如一个 Linux/UNIX 系统采取了以上各种安全措施，那么攻击者要想侵入系统，将不得不绕过防火墙，避开入侵检测系统，跳过陷阱程序，通过系统过滤器，逃过日志监视器，修改文件系统属性，破坏安全登录服务器才能最终达到目的。由于其中任何一个环节都可能激发报警，因此，入侵者要想侵入这样的系统而又不被发现几乎是不可能的。

操作系统安全关系到所有应用系统的安全，也关系到整个网络安全的基础。本章分析了安全操作系统的发展历史，分析了操作系统的安全机制，重点对 Linux、Windows 2000/2003 和 UNIX 主流操作系统的安全进行了分析，并提供了安全加固的方法。还提供了有关如何解决 Linux、Windows 和 UNIX 的网络操作系统上发现的特定漏洞的指导。提供了有关特定对策可能如何影响计算机的功能、可管理性、性能和可靠性的信息，以便用户可以明智地选择在自己的环境中实施哪些对策。通过本章的学习，用户将可在一定程度上提高操作系统的安全性。但需要注意的是，一但发现严重安全漏洞时，先前配置的环境可能再次受到攻击。所以，需要管理员监视各种资源以便及时了解与操作系统、应用程序和设备相关的安全问题。这一点至关重要，因为没有哪个网络服务器是绝对安全的。务必理解保护网络中的服务器的任务不是一次性工程，而是一个在其预算和日程中包括的持续过程。每个组织应将安全性视为优先级别最高的事务之一。

## 习 题 4

(1) 什么是安全操作系统？简单说明 TCSEC 的主要内容。

（2）Linux 操作系统是如何实行配额和限制的，为什么要这样做？
（3）Windows Server 2003 如何进行安全基线的配置？
（4）找出 Linux 系统与 Windows 操作系统有关安全配置上的共同点和不同点。
（5）操作系统的安全威胁有哪些？
（6）简述操作系统安全设计的基本原则。
（7）简述 Linux/UNIX 的安全策略。
（8）简述 NTFS 文件系统的安全性。

# 第 5 章 chapter 5

# 网络应用系统的安全策略

当谈到网络应用安全的时候，许多企业及学校仅仅扫描系统漏洞就应付了事，这样是错误的。网络应用是恶意和非法进入组织机构网络的最佳入口。最小的系统加最少的应用服务，相对来说是比较安全的。网络平台的系统安全性和网络应用的安全性是截然不同的概念。因此，需要认真对待每个网络应用，了解入侵是如何发生的，学习如何在他人找到网络安全防护漏洞之前修补破绽，保护网络应用系统的安全。下面列出的是需要注意的三大网络应用安全问题。

## 5.1 网络应用安全概述

### 5.1.1 身份验证

身份验证是网络应用安全最重要的阶段，即使使用 SSL 或强大的两次验证机制（如用户 ID 和复杂的密码）也是如此。存在缺陷的凭证管理任务，包括密码修改、用户信息更新和其他相关的功能，能够削弱验证的效果。因此，即使使用者拥有有效的会话权限，依然需要重新验证所有的账号管理任务。

对于大部分网络应用，用户验证包括用户 ID 和密码两部分。强大的验证方法随处可见，既有基于软件或者硬件的密码验证，也有生物学验证方法。

这些方法虽然为应用增加了成本，但仍然应该坚持将这些成本归入开发过程。如果在劝说当权者时遇到阻力，可以考虑用案例来说服他，联邦储蓄保险公司（FDIC）在 2000 年就宣布，由于身份窃贼问题的严重化，网上银行有义务进行多重验证（如硬件/软件加密或生物学验证），对传统的两重验证进行补充。

### 5.1.2 访问控制

访问控制是网络应用使用验证方法来接受或拒绝对内容和功能访问的过程。以下是两种主要的访问控制方法。

路径挖掘：恶意用户会将相关路径信息（如 https://your_Website.com/target_dir/target_file）作为对素材的直接申请进行路径挖掘攻击。此类攻击企图访问一般无法直

接访问的文件。借助网络浏览器、系统呼叫和 shell 命令、URL 或使用黑客工具进行袭击。

客户端缓存：默认情况下，大部分的网页浏览器都会缓存网络页面。入侵者可以利用缓存信息访问安全地址。用户频繁使用公用或者共享计算机通过网络应用访问信息。因此，网络应用应该包括限制缓存敏感信息的功能，以防止在浏览器中缓存用户信息。

### 5.1.3 未授权的输入

网络应用响应用户的 HTTP 请求，袭击者修改 HTTP 的请求（如 URL 或对后端数据库进行查询的字符串、表单域、隐藏域等）来绕过网站的安全机制。最常见的袭击后果是跨站脚本、缓存溢出以及资料隐码。

单纯依靠客户端机制验证输入的网站只考虑到了网站的性能和可用性。入侵者能轻易地绕过检验机制，使得缺乏保护的网络应用要面对恶意的输入。

黑客们使用工具生成自己的 HTTP 请求来绕过网络浏览器的验证机制。服务器端的验证是防止此类利用 HTTP 请求进行入侵的必需的手段。

### 5.1.4 应采取的措施

如果网络应用本身存在许多固有的不安全性，包含如此多的危险，那么如何确保安全？答案相对来说很简单。

在应用建立的过程中，编码文档的建立以及独立的编码审查就是成功实现安全的关键。记录每行语句，并寻求擅长应用安全的第三方对系统以及升级应用所使用的控制方式进行评估。

如果已经在线发布网络应用，且忘记做安全工作，那也不算太晚——你依然能够保护应用的安全。即使在发布之前进行过大范围的编码审查，还应该继续进行查找安全裂缝和缺陷的测试以及应用维护。

在进行网络应用安全测试时，可以有多种选择。如果不知道应该如何进行安全测试，可以使用网络应用安全工具。

在实施某个应用时，人们（包括公司内部人员以及外部人员）是最好的应用测试员。在全部应用实施之前，以及主要应用进行修改之时，都要继续进行应用缺陷和渗透性测试。系统安全检查只能提供关于平台安全的信息，需要采取额外措施来确保应用的安全。

## 5.2 电子邮件系统安全策略

电子邮件（E-mail）是通过 Internet 或者 Intranet 等网络，从终端机输入文件、图片或者声音等，通过邮件服务器传送到另一端的终端机上的信息。电子邮件是目前人们在虚拟网络空间中使用频率最高的通信方法。

随着国内 Internet 的发展，电子邮件作为一种通信方式逐渐普及。当前电子邮件的

用户已经从教育领域发展到了普通家庭中，电子邮件传递的信息也从普通文本信息发展到包含声音、图像在内的多媒体信息。随着用户的增多、使用范围的逐渐扩大，保证邮件本身的安全以及电子邮件对系统安全性的影响越来越重要。

现在电子邮件基本上都是基于 TCP/IP 协议的。在 TCP/IP(IPv4)协议簇中，TCP 协议对电子邮件通信双方的身份认证依赖于 IP 包中的源地址和目的地址。电子邮件在 Internet 上是以明文形式传递的，窃听者可以截获 IP 包，从中分析出源地址、目的地址以及邮件的内容。一旦窃听者掌握了通信双方的地址信息就可以假冒任意一方，重新启动与另一方的通信，邮件内容也会以明文的形式泄露。

当用户从当地的邮件服务器上收取电子邮件时，服务器会要求用户输入账号及密码，以确认用户的合法身份。但用户输入的账号和密码是以明文形式通过网络传递给服务器的，窃听者只要监听到客户和服务器在这一次应答过程中交换的数据包，就可以获得客户的账号和密码，从而完全获得用户邮箱内的邮件及其内容，用户就毫无秘密可言。现在很多的电子邮件产品，在安全性方面各有其缺点。

PGP(pretty good privacy)是近几年应用于保密电子邮件的一个性能很好的软件。它能够对邮件发送者身份的认证，对 E-mail 消息加密以及对 E-mail 明文消息的完整性进行校验。它的密钥管理采用了以 RSA 公开密钥算法传送密钥，但没有采用证书管理体制；数据加密采取了 IDEA(国际数据加密标准)，加解密速度比较快；MD5 用作单向 Hash 函数，通过使用 RSA 加密算法用邮件发送者的秘密密钥，对 E-mail 消息的 MD5 消息摘要进行加密实现数据完整性校验。

尽管 PGP 应用公开密钥、单钥、Hash 等算法实现了二级密钥管理，但它的密钥管理依旧存在缺陷——缺少第三方对通信双方身份的认证。这给 PGP 的安全性造成了极大的威胁。公钥的鉴别模仿现实生活中人们的相互信任关系，划分成 5 级信任度，信任度存在递减问题。其次，假设用户 A 和 B 第 1 次使用 PGP 进行通信，而 B 要将其公钥发送给 A，如果通过电子邮件传送，也只能以明文形式传递。如果攻击者 T 截获 B 的公钥，然后将自己的公钥，取代 B 的公钥发送给 A，于是 T 假冒了 B，从而导致 A 发给 B 的信息被攻击者 T 收取并阅读，而 A 却无法察觉。由于 PGP 在运行过程中使用了一些存储块，而在使用 PGP 的清除功能后，却没有真正地将数据从存储块上清除掉，这给密码分析者留下了寻找密钥的可能途径；PGP 重新运行时，可能会重复使用存储块的数据。再者，PGP 的随机数产生方式也不是太理想，它是通过测试用户击键的时间间隔来产生随机数，随机数的产生完全由软件来实现，如果程序被修改，很可能产生的随机数不具有随机性；随机数种子是以文件形式存放在用户的存储空间中，文件的安全问题会导致整个系统安全性能的削弱。

保密电子邮件涉及 SMTP、POP3 协议和 PEM 标准。

简单邮件传输协议(simple mail transport protocol，SMTP)负责电子邮件在网络上的传递。SMTP 协议规定了邮件怎样在邮件服务器中传递，已经成为目前互联网上邮件传输的标准。但是从安全的角度上 SMTP 几乎是不设防的协议，SMTP 的消息传输采用的是明文形式而且固定在 25 端口，所以易被监听和攻击。

邮局协议版本 3(post office protocol 3，POP3)规定了用户怎样从邮件服务器上收取

邮件。用户在使用 POP3 协议收取邮件时需要进行身份确认，认证成功后向用户传递邮件，但这并不意味着 POP3 就是安全的。事实上，POP3 协议提供的安全很有限，因为它只是提供了对用户的身份保护，并没有提供对邮件内容的加密措施。如果窃密者使用被动供给技术则可以绕过身份确认直接得到电子邮件的明文。

由以上协议的安全性分析可知，传统的电子邮件系统无论是邮件的网络传输，还是客户和邮件服务器之间的交互都存在着巨大的安全隐患。

### 5.2.1 SMTP 协议的安全性问题

在 Internet 中，E-mail 是通信双方通过其在运输层的 25 号端口建立的连接来进行的。侦听 25 号端口的就是 SMTP，它是一个后台进程，由它去接受连接请求，并将报文送入相应的邮箱中。连接建成后，发送方按客户方式运行，而接收方按服务器方式运行。客户要等待服务器的响应，直到服务器能够接受 E-mail 时，才开始发送。首先发送方要宣布自己是谁，发信给谁。当服务器认定收信者确有其人时，就通知发送方可以发信过来。接着就进入发送方发报文、服务器接收报文以及确认接受的过程，一直到发完报文，释放连接为止。

E-mail 用户的唯一标识是邮件地址，如 Username@domain. com，即名为 Username 的用户使用域名为 domain. com 的邮件服务器进行邮件的发送和接收。用户通常可使用客户端软件(Foxmail、Outlook Express 等)联系服务器进行邮件收发。客户将邮件提交给邮件服务器之后，还需要邮件服务器进行一系列复杂的传递操作，这才能将邮件传送到目的地址所在的邮件服务器。这一传递过程的实现就依赖于 SMTP 服务，SMTP 定义了一套有效的传递规则，它以协议的方式规定了网络中全部邮件服务器必须遵守的准则。

电子邮件服务除了依赖于 SMTP 协议之外，还需要 POP 协议的支持，而 POP 协议是 IIS 所不能支持的，所以，使用 IIS 服务器并不能实现完整的邮件服务。笼统地说，SMTP 负责邮件的传递，从客户机到邮件服务器以及服务器之间的传递工作。而 POP 协议能够让客户检索到由 SMTP 发送来的邮件，并将此邮件下载到用户本地。

#### 1. SMTP 模型、命令及规范

如图 5-1 所示，SMTP 模型在工作时，首先由用户发送请求给发送端 SMTP 服务器，然后发送端 SMTP 服务器与接收端 SMTP 服务器建立双向传输通道。此处接收端 SMTP 服务器可能是最终接收端，也可能是中间转发接收端。双向通道建立起来之后，接收端和发送端 SMTP 服务器就按协议规定的命令进行应答。

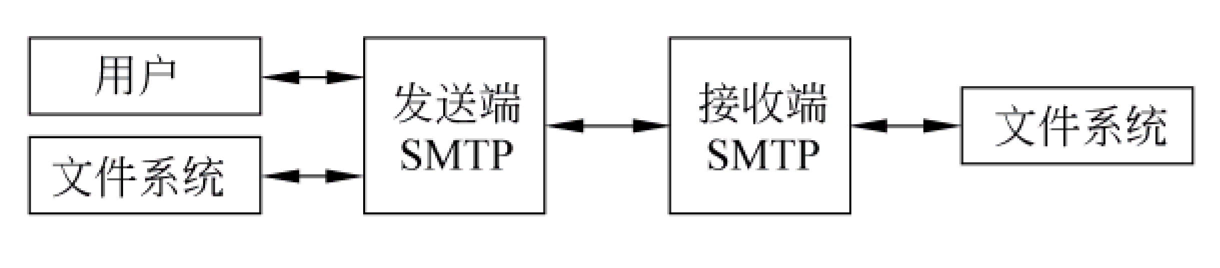



**图 5-1　SMTP 模型**

SMTP 协议中规定的命令有 MAIL、RCPT、DATA、VRFY、EXPN、SEND、SOML、SAML、HELO、QUIT、RSET、HELP、NOOP 等。其中 HELO、MAIL、RCPT、DATA、RSET、NOOP、QUIT 7 条命令组成了 SMTP 协议的最小命令集。

**2. SMTP 协议原理**

SMTP 是一组由源地址到目的地址传送邮件的规则，由它来控制信件的中转方式。SMTP 协议属于 TCP/IP 协议簇，它帮助每台计算机在发送或中转信件时找到下一个目的地。通过 SMTP 协议所指定的服务器，就可以把 E-mail 寄到收信人的服务器上，整个过程只要几分钟。SMTP 服务器则是遵循 SMTP 协议的发送邮件服务器，用来发送或中转用户发出的电子邮件。SMTP 协议规定命令是以明文方式传递的。

SMTP 工作在两种情况下：一是电子邮件从客户机传输到服务器；二是从某一个服务器传输到另一个服务器。

SMTP 是请求/响应协议，命令和响应都是基于 ASCII 文本，并以 CR 和 LF 符结束。响应包括一个表示返回状态的三位数字代码。

SMTP 在 TCP 协议 25 号端口监听连接请求。

连接和发送过程如下。

(1) 建立 TCP 连接。

(2) 客户端发送 HELO 命令以标识发件人自己的身份，然后客户端发送 MAIL 命令，服务器端以 OK 作为响应，表明准备接收。

(3) 客户端发送 RCPT 命令，以标识该电子邮件的计划接收人，可以有多个 RCPT 行，服务器端则表示是否愿意为收件人接受邮件。

(4) 协商结束，发送邮件，用命令 DATA 发送。

(5) 以“.”表示结束输入内容一起发送出去。

(6) 结束此次发送，用 QUIT 命令退出。

另外两个命令的功能如下。

VRFY：用于验证给定的用户邮箱是否存在，以及接收关于该用户的详细信息。

EXPN：用于扩充邮件列表。

邮件路由过程如下。

SMTP 服务器基于域名服务 DNS 中计划收件人的域名及 MX 记录来路由电子邮件。MX 记录注册了域名和相关的 SMTP 中继主机，属于该域的电子邮件都应向该主机发送。

若 SMTP 服务器 mail.abc.com 收到一封信要发到 shuser@sh.abc.com：

(1) Sendmail 请求 DNS 给出主机 sh.abc.com 的 CNAME 记录，如果有，假设 CNAME 到 shmail.abc.com，则再次请求 shmail.abc.com 的 CNAME 记录，直到没有为止。

(2) 假定被 CNAME 到 shmail.abc.com，然后 Sendmail 请求@abc.com 域的 DNS 给出 shmail.abc.com 的 MX 记录。

```
shmail MX 5 shmail.abc.com
```

```
10 shmail2.abc.com
```

(3) Sendmail 最后请求 DNS 给出 shmail.abc.com 的 A 记录,即 IP 地址,如返回值为 1.2.3.4。

(4) Sendmail 与 1.2.3.4 连接,传送这封给 shuser@sh.abc.com 的信到 1.2.3.4 这台服务器的 SMTP 后台程序。

怎样由信封部分检查一封信是否是伪造的?

(1) 检查 received 行的关联性。

现在的 SMTP 邮件传输系统,在信封部分除了两端的内部主机处理之外,还考虑两个公司防火墙之间的部分。若两台防火墙机器分别为 A 和 B,但接收者检查信封 received 行时发现经过了 C 则是伪造的。

(2) 检查 received 行中的主机和 IP 地址对是否对应。

```
Received: from galangal.org (turmeric.com [104.128.23.115] by mail .bieberdorf.edu …
```

(3) 检查被手动添加在最后面的 received 行。

```
Received: from galangal.org ([104.128.23.115]) by mail .bieberdorf.edu (8.8.5)
Received: from lemongrass.org by galangal.org (8.7.3)
Received: from graprao.com by lemongrass.org (8.6.4)
```

#### 3. SMTP 安全性分析

SMTP 协议没有采用任何安全机制,全部信息采用明文形式传送,并且采用固定的端口号 25 进行邮件的发送,攻击者只要监听端口号 25 的数据流,就能分析出 SMTP 命令及其参数内容,进而达到分析出所有邮件内容的目的。

在发送邮件的过程中,MAIL 和 RCPT 命令都可能被监听,分析其参数获知邮件的来源和去向。攻击者一旦掌握了这些信息,就可能采取假冒攻击。

VRFY 和 EXPN 命令也可能被监听,攻击者可以掌握用户和邮箱地址,进而进行假冒攻击。

DATA 命令很可能成为主动攻击的介入点。攻击者截获 DATA 命令,然后用自己伪造的邮件内容代替原有邮件内容发送给接收者,即进行假冒攻击。

TURN 命令可以使收发双方角色互换,攻击者利用这一命令可以逃避邮件过滤防火墙的检查,让不允许外出的邮件出去,不允许进来的邮件进来,从而使过滤防火墙失去其应有功能。

通过对 reverse-path 的修改,可以直接导致邮件误投,邮件被错误地导入攻击者的邮箱。

### 5.2.2 Sendmail 服务器的安全问题

由于程序设计上的缺陷,加上功能配置非常复杂,Sendmail 往往成为系统安全的隐患。当然,可以先建一个宏配置文件,然后使用 m4 宏预处理器生成主配置文件,这样就变得相对容易。但是,要掌握所有的配置选项不是一件容易的事情。Sendmail 在过去的

版本中出现过很多安全漏洞,促使管理员不得不赶快升级版本。而且 Sendmail 的流行性也使其成为攻击的目标,这意味着安全漏洞可以很快被发现,但同时也使得 Sendmail 更加稳定和安全。另外一个问题是 Sendmail 的一般默认配置都具有最小的安全特性,从而使 Sendmail 往往容易被攻击。如果使用 Sendmail,应该确保理解每个打开选项的含义及影响。一旦理解了 Sendmail 的工作原理,Sendmail 的安装和维护就变得非常容易了。通过 Sendmail 的配置文件,用户可以完成一切想要得到的需求。

**Sendmail 的安全配置**

Sendmail 作为免费的邮件服务器软件,已被广泛应用于 Internet 各种操作系统的服务器中。如 Solaris、HPUX、AIX、IRIX、Linux 等。随着互联网的普及,邮件服务器受攻击的机会也大大增加。目前互联网上的邮件服务器所受攻击主要有两类:一类就是中继利用(Relay),即远程机器通过你的服务器来发信,这样任何人都可以利用你的服务器向任何地址发邮件,久而久之,你的机器不仅成为发送垃圾邮件的帮凶,也会使网络国际流量激增,同时可能被网上的很多邮件服务器所拒绝;另一类攻击称为垃圾邮件(Spam),即人们常说的邮件炸弹,是指在很短时间内服务器可能接收大量无用的邮件,从而使邮件服务器不堪负载而出现瘫痪。这两种攻击都可能使邮件服务器无法正常工作,因此,作为一个邮件服务器,防止邮件攻击将不可缺少。

目前,Sendmail 邮件服务器阻止邮件攻击的方法有两种:一种是升级高版本的服务器软件,利用软件自身的安全功能;第二种就是采用第三方软件,利用其动态中继验证控制等功能来实现。

下面就以 Sendmail 8.9.3 为例,介绍一下使用方法。

1) 服务器自身安全功能

要利用 Sendmail 8.9.3 的阻止邮件攻击功能,就必须在系统编译时对相关参数进行设置,并借助相关的软件包。目前主要就是利用 Berkeley DB 数据库的功能,Berkeley DB 包可以从相关站点上下载,并需要预先编译好。然后将 Berkeley DB 的相关参数写进 Sendmail 的有关文件中。

将编译好的 Berkeley DB 有关库文件路径加入到 site. config. m4 文件中,使 Sendmail 编译后能够使用 Berkeley DB 数据库。

```
# cd $ /sendmail-8.9.3/BuidTools/Site
```

修改 site. config. m4 文件

```
define (confINCDIRS, -I/usr/local/BerkeleyDB/include)
define (confLIBDIRS, L/usr/local/BerkeleyDB/lib)
```

Sendmail. mc 是生成 Sendmail. cf 的模板文件之一,要使 Sendmail 具有抗邮件攻击功能还需在该文件中进行相关定义。主要包括以下几项:

```
FEATURE (relay_entire_domain)
FEATURE (ACCESS_DB) dnl
FEATURE (blacklist_recipients)
```

正确编译好 Sendmail 是邮件服务器安全控制的基础,而真正的安全设置主要还是利用相关文件进行的。这种包含控制语句的文件主要是 access 和 relay-domains。

access 是邮件安全控制的主要数据库文件,在该文件中可以按照特定的格式将需控制的域名、IP 地址或目标邮件地址,以及相应的动作值写入,然后使用 makemap 命令生成 access.db 文件。

```
# makemap hash access.db
spam.com REJECT
edu.cn OK
hotmail.com DISCARD
```

其中,REJECT 动作是拒绝接受从指定地址发来的邮件;OK 是允许特定地址用户任意访问;relay 是允许通过本邮件服务器进行中转邮件;DISCARD 是将收到的邮件交给特定命令进行处理,例如,可以设定将收到的邮件丢弃,或者设定收到邮件后返回给使用者一条出错信息等。

Relay-domains 文件是设定哪些域是该服务器可以中继的域,其格式为每个域占一行。

```
…
CN
EDU
JP
…
```

在服务器开始使用时建议将所有顶级域名加入其中,以后再根据安全需要对其进行修改,否则将会使 POP3 用户发送邮件时出现 relay reject 错误,而无法向没有加入的域名目标邮件地址发送邮件。

2) relay 规则限制

RedHat 7.2 自带了 Sendmail 8.11.6,默认 Sendmail 只监听 127.0.0.1 地址,而且只对本机转发。这的确非常安全,可是外面的机器根本无法连接到主机的 25 号端口,合法的客户也不能使用 SMTP 服务。所以首先需要修改/etc/sendmail.cf 文件,找到如下行:

```
O DaemonPortOptions=Port=smtp, Addr=127.0.0.1, Name=MTA
```

删除 Addr=127.0.0.1,然后重启 Sendmail。

```
/etc/rc.d/init.d/sendmail restart
```

这样 Sendmail 可以监听 0.0.0.0 地址,即所有的机器都可以连接了。可是用主机作 SMTP 服务器发信时,如果发送者和接收者都不是本地域,则会提示 Relaying denied。这是因为 Sendmail 默认允许对本机进行转发,而使用 Access Map 进行转发规则的管理。

Sendmail 检查/etc/mail/relay-domains 文件,决定是否转发邮件,它通过判断设置的 IP 地址或域名决定是否允许转发。如果/etc/mail/relay-domains 文件不存在或这一步不允许,Sendmail 还会再检查/etc/mail/access 文件。

Access 文件分两个部分：左边是入口，可以是域名、E-mail 地址、本地用户名部分和 IP 地址；右边是操作标记。

OK　　接收 E-mail，即使被其他规则拒绝了。

RELAY　　允许通过该邮件主机转发的域，转发意味着 OK。

REJECT　　拒绝 E-mail 并且显示内部通过的错误提示。

DISCARD　　安静地接收随后取消掉这封邮件。

XYZ some other text　　XYZ 是 RFC821 兼容的错误代码，后面是自定义的错误信息。

下面是一个/etc/mail/access 的样例。

```
localhost.localdomain          RELAY
localhost                      RELAY
127.0.0.1                      RELAY
192.168.1.1                    RELAY
```

它除了对本机转发，还对内网的 192.168.1.1 地址进行转发。若使每一次的修改有效，必须重新生成 access 的数据库文件，执行如下命令：

```
#makemap-v hash /etc/mail/access < /etc/mail/access
```

现在 192.168.1.1 就可以使用主机任意发送邮件了。

3）本地安全性配置

smrsh 程序的目的是作为在 mailer 中为 Sendmail 定义/bin/sh 的替代 shell。smrsh 是一种受限 shell 工具，它通过/etc/smrsh 目录来明确指定可执行文件的列表。简而言之，smrsh 限制了攻击者可以执行的程序集。当它与 Sendmail 程序一起使用的时候，smrsh 有效地将 Sendmail 可以执行程序的范围限制在 smrsh 目录中。

方法如下：

```
# cd /etc/smrsh
# ln -s /bin/mail mail
# ln -s /usr/bin/procmail procmail
```

这将允许位于.forward 和 aliases 中的用户采用管道符语法 program 来运行 mail 及 procmail 程序。

mailer 程序在 Sendmail 的配置文件/etc/sendmail.cf 中仅有一行。必须修改 sendmail.cf 文件中 Mprog 定义的那一行，将/bin/sh 替换为/usr/sbin/smrsh。这样，Sendmail 就使用受限 shell，增加了本地安全性。

修改 sendmail.cf 文件如下：

```
Mprog, p=/bin/sh …
```

将其改为：

```
Mprog, p=usr/sbin/smrsh …
```

重启 Sendmail 使之生效：

```
# /etc/rc.d/init.d/sendmail restart
```

如果没有加以正确和严格的管理的话，别名文件被用来获取特权。例如，很多发行版本在别名文件中带有 decode 别名，现在这种情况越来越少了。

这样做的目的是为用户提供一个通过 mail 传输二进制文件的方便方式。在邮件的发送地，用户把二进制文件用 uuencode 转换成 ASCII 格式，并把结果邮递给接收地 decode 别名。别名通过管道把邮件消息发送到/usr/bin/uuencode 程序，由这个程序来完成从 ASCII 转回到原始的二进制文件的工作。

类似地，对于所有用于执行没有被放在 smrsh 目录下的程序的别名，都要仔细地检查，可能它们都值得怀疑并应当删除。要想使改变生效，需要运行：

```
# /usr/bin/newaliases
```

编辑别名文件（vi /etc/aliases）并删除以下各行：

```
# Basic system aliases -- these MUST be present
MAILER-DAEMON: Postmaster
postmaster: Root
# General redirections for pseudo accounts
bin: Root
daemon: Root
games: Root          删除这一行
ingres: Root         删除这一行
nobody: root
system: root         删除这一行
toor: root           删除这一行
uucp: root           删除这一行
# Well-known aliases
manager: root        删除这一行
dumper: root         删除这一行
operator:: root      删除这一行
# trap decode to catch security attacks
decode: root         删除这一行
# Person who should get root's mail
# root: marc
```

最后应该运行/usr/bin/newaliases 程序使改动生效。

最新版本的 Sendmail 8.9.3 加入了很强的防止欺骗的特性。它们可以防止邮件服务器被未授权的用户滥用。编辑/etc/sendmail.cf 文件，修改一下配置文件，使邮件服务器能够挡住欺骗邮件。

编辑 sendmail.cf 文件（vi /etc/sendmail.cf）并更改下面一行：

```
O PrivacyOptions=authwarnings
```

改为：

```
PrivacyOptions=authwarnings, noexpn, novrfy
```

设置 noexpn 使 Sendmail 禁止所有 SMTP 的 EXPN 命令，它也使 Sendmail 拒绝所有 SMTP 的 VERB 命令。设置 novrfy 使 Sendmail 禁止所有 SMTP 的 VRFY 命令。这种更改可以防止欺骗者使用 EXPN 和 VRFY 命令，而这些命令恰恰被那些不守规矩的人所滥用。

当 Sendmail 接受一个 SMTP 连接的时候，它会向那台机器发送一个问候信息，这些信息作为本台主机的标识，而且它所做的第一件事就是告诉对方它已经准备好了。

编辑 sendmail. cf 文件(vi /etc/sendmail. cf)并更改下面一行：

```
O SmtpGreetingMessage=$ j Sendmail $ v/$ Z; $ b
```

改为：

```
O SmtpGreetingMessage=$ j Sendmail $ v/$ Z; $ b NO UCE C=xx L=xx
```

现在手工重启一下 Sendmail 进程，使刚才所做的更改生效：

```
# /etc/rc.d/init.d/sendmail restart
```

以上的更改将影响到 Sendmail 在接收一个连接时所显示的标志信息。应该把 C=xx L=xx 条目中的 xx 换成所在的国家和地区代码。

通常情况下，任何人都可以使用 mailq 命令来查看邮件队列的内容。为了限制可以审核邮件队列内容的人员，只需要在/etc/sendmail. cf 文件中指定 restrictmailq 选项即可。在这种情况下，Sendmail 只允许与这个队列所在目录的组相同的用户可以查看它的内容，允许权限为 0700 的邮件队列目录被完全保护起来，而限定的合法用户仍然可以看到它的内容。

编辑 sendmail. cf 文件(vi /etc/sendmail. cf)并更改下面一行：

```
O PrivacyOptions=authwarnings, noexpn, novrfy
```

改为：

```
O PrivacyOptions=authwarnings, noexpn, novrfy, restrictmailq
```

现在更改邮件队列目录的权限使它被完全保护起来：

```
# chmod 0700 /var/spool/mqueue
```

**注意**：已经在 sendmail. cf 中的“PrivacyOptions=”行中添加了 noexpn 和 novrfy 选项，现在在这一行中接着添加 restrictmailq 选项。

任何一个没有特权的用户，如果试图查看邮件队列的内容会收到下面的信息：

```
$ /usr/bin/mailq
You are not permitted to see the queue
```

限制处理邮件队列的权限为 root。通常，任何人都可以使用-q 开关来处理邮件队列，为限制只允许 root 处理邮件队列，需要在/etc/sendmail. cf 文件中指定 restrictqrun。

编辑 sendmail.cf 文件(vi /etc/sendmail.cf)并更改下面一行：

```
O PrivacyOptions=authwarnings, noexpn, novrfy, restrictmailq
```

改为：

```
O PrivacyOptions=authwarnings, noexpn, novrfy, restrictmailq, restrictqrun
```

任何一个没有特权的用户,如果试图处理邮件队列的内容会收到下面的信息：

```
$ /usr/sbin/sendmail -q
You do not have permission to process the queue
```

可以通过使用 chattr 命令使重要的 Sendmail 文件不会被擅自更改,可以提高系统的安全性。具有"+I"属性的文件不能被修改：它不能被删除和改名,不能创建到这个文件的链接,不能向这个文件写入数据。只有超级用户才能设置和清除这个属性。

为 sendmail.cf 文件设置不可更改位：# chattr+i /etc/sendmail.cf

为 sendmail.cw 文件设置不可更改位：# chattr+i /etc/sendmail.cw

为 aliases 文件设置不可更改位：# chattr+i /etc/aliases

为 access 文件设置不可更改位：# chattr+i /etc/mail/access

为 null.mc 文件设置不可更改位：# chattr+i /etc/null.mc

为 sendmail.mc 文件设置不可更改位：# chattr+i /etc/sendmail.mc

从 8.9 版本开始,默认的是不允许邮件转发的。最简单的允许邮件转发的方法是在文件/etc/mail/relay-domains 中进行设置。该文件中列出的域名的信件都允许通过本地服务器进行邮件转发。

为了更精确的设置,可以在 sendmail.mc 中添加如下几个参数允许被用来设置邮件转发。

FEATURE(relay_hosts_only)：通常情况下,在文件/etc/mail/relay-domains 中列出域名的主机都允许通过本地机转发,而该设置指定必须罗列出每个允许通过本机转发邮件的主机。

FEATURE(relay_entire_domain)：该参数指示允许所有本地域通过本机进行邮件转发。

FEATURE(access_db)：该参数指定利用散列数据库/etc/mail/access 来决定是否允许某个主机通过本地进行邮件转发。

FEATURE(blacklist_recipients)：若该参数被设置,则在决定是否允许某个主机转发邮件的同时察看邮件发送地址和邮件目的地址。

FEATURE(rbl)：允许基于 maps.vix.com 由黑名单(Realtime BlackholeList)进行邮件拒绝,防范垃圾邮件。

FEATURE(accept_unqualified_senders)：允许接受发送者地址不包括域名的邮件,例如 user,而不是 user@C.NET。

FEATURE(accept_unresolvable_domains)：通常来讲,Sendmail 拒绝接受发送者邮件地址指定的主机通过 DNS 不能解析的邮件,而该参数允许接收这种邮件。

FEATURE(relay_based_on_MX)：该参数允许转发邮件接受者地址的 MX 记录指向本地的邮件。例如，本地接收到一个发送目的地址为 user@b.com 的邮件，而 b.com 域名的 MX 记录指向了本地机器，则本地机器就允许转发该邮件。

下面几个特性可能会有安全漏洞，一般当邮件服务器位于防火墙后面时才能使用，因为这些参数可能导致系统易于被垃圾邮件发送者利用。

FEATURE(relay_local_from)：该参数指定若消息自称源于本地域，则允许转发该邮件。

FEATURE(promiscuous_relay)：打开对所有的邮件的转发。

宏配置文件“sendmail.mc”设置成功以后，可以用下面的命令创建 Sendmail 的配置文件：

```
# cd /var/tmp/sendmail-version/cf/cf/
# m4 ../m4/cf.m4 /etc/sendmail.mc> /etc/sendmail.cf
```

**注意**：这里“../m4/cf.m4”是告诉 m4 程序的默认配置文件路径。

## 5.2.3 POP 协议的安全问题

POP3 协议，即邮局协议版本 3，RFC1939 详细描述了其规范和命令。与 SMTP 协议相对应，POP3 协议用于收取电子邮件。

POP 协议是一种允许用户从邮件服务器收发邮件的协议，使用固定的端口号 110 进行邮件的收取。它说明 PC 如何与 Internet 上的邮件服务器连接及如何下载 E-mail。POP 协议负责将邮件通过 SLIP/PPP 连接传送到用户的主机上。它只负责接收，不能通过它发送邮件。通常来说，POP 协议有 2 个版本，即 POP2 和 POP3，都具有简单的电子邮件存储转发功能。POP2 与 POP3 本质上类似，都属于离线式工作协议，但是由于使用了不同的协议端口，因此，两者并不兼容。本节将探讨 POP 协议的安全问题。

### 1. POP 协议的工作原理

一般来说，人们习惯称呼 POP 协议为 POP 服务器。目前在 Internet 上的大多数 POP 服务器为 POP3 服务器。POP3 协议与 SMTP 协议相结合，是目前最常用的电子邮件服务协议。SMTP 服务器将邮件发送给 POP3 服务器。用户使用客户端邮件软件联系 POP3 服务器，使用账号和密码进行身份验证之后，用户将待发邮件从本地发送到服务器。POP3 服务器将用户邮件发送到用户本地。这一过程中，POP3 服务器本身也是一台 SMTP 服务器，但它能够为每一用户指定一个单独的文件夹，这是纯粹的 SMTP 服务器所不能做到的。

POP3 除了支持离线工作方式外，还支持在线工作方式。在离线工作方式下，用户收发邮件时，首先，通过 POP3 客户端程序登录到支持 POP3 协议的邮件服务器，然后发送邮件及附件。其次，邮件服务器将为该用户收存的邮件传送给 POP3 客户程序，并将这些邮件从服务器上删除。最后，邮件服务器将用户提交发送的邮件，转发到运行 SMTP 协议的计算机中，通过它实现邮件的最终发送。在为用户从邮件服务器收取邮件时，POP3 是以该用户当前存储在服务器上的全部邮件为对象进行操作的，并一次性将它们

下载到用户计算机中。一旦客户的邮件下载完毕，邮件服务器对这些邮件的暂存托管即告完成。使用 POP3，用户不能对他们储存在邮件服务器上的邮件进行部分传输。离线工作方式适合那些从固定计算机上收发邮件的用户使用。

当使用 POP3 在线工作方式收发邮件时，用户是在所用的计算机与邮件服务器保持连接的状态下读取邮件的。用户的邮件保留在邮件服务器上。

### 2. POP3 协议安全性分析

与 SMTP 协议一样，POP3 协议也具有明文传送数据的不安全性因素。例如，user/pass 命令就是一个严重的漏洞，攻击者很容易窃听到用户名和密码。一旦密码暴露，用户的一切邮件将完全展现在攻击者面前。尽管 POP3 协议提供了一个 APOP 命令，用于对用户身份的认证，具有一定的安全性，但其提供的安全性能却是有限的和不完善的。

该命令仅对用户名和密码加密，可以对用户身份的认证起到一定的保护作用，而对邮件的内容则毫无保护作用，无法抵御被动攻击，即使攻击者不知道用户密码，也能监听到以明文形式传递的邮件内容。

对用户名和密码的安全性而言，这条命令的作用也有限，因为根据 APOP 命令的安全机制，要保证用户名和密码的安全性，就必须保证 POP3 客户端和服务器端共知的一个秘密字符串的安全性。一旦这一字符串泄露，则 APOP 命令就毫无安全性可言了。

RETR 和 TOP 命令都可以查看邮件内容。在邮件内容传递过程中，攻击者可以采取被动攻击，窃听邮件的内容。甚至可以采取主动攻击，修改邮件内容，欺骗接收端用户，或根据邮件的内容，假冒接收端用户欺骗发送端用户。

### 3. 常用的 POP3 命令

表 5-1 列出了常用的 POP3 命令。

**表 5-1 常用的 POP3 命令**

| 命令 | 参数 | 状态 | 描述 |
|---|---|---|---|
| USER | Username | 认可 | 此命令与下面的 PASS 命令若成功，将导致状态转换 |
| PASS | Password | 认可 | |
| APOP | Name、Digest | 认可 | Digest 是 MD5 消息摘要 |
| STAT | None | 处理 | 请求服务器发回关于邮箱的统计资料，如邮件总数和总字节数 |
| UIDL | [msg＃] | 处理 | 返回邮件的唯一标识符，POP3 会话的每个标识符都将是唯一的 |
| LIST | [msg＃] | 处理 | 返回邮件数量和每个邮件的大小 |
| PETR | [msg＃] | 处理 | 返回由参数标识的邮件的全部文本 |
| DELE | [msg＃] | 处理 | 服务器将由参数标识的邮件标记为删除，由 quit 命令执行 |
| RSET | None | 处理 | 服务器将重置所有标识为删除的邮件，用于撤销 DELE 命令 |
| TOP | [msg＃] | 处理 | 服务器将返回由参数标识的邮件前 n 行内容，n 必须是正整数 |
| NOOP | None | 处理 | 服务器返回一个肯定的响应，不做任何操作 |
| QUIT | None | 更新 | 退出 |

这 12 条命令可分为 3 组，表 5-2 列出了不同状态下可用的不同命令。

**表 5-2 POP3 状态——命令对照表**

| 状态 | 可用命令集 |
|---|---|
| 验证态 | USER、PASS、APOP、QUIT |
| 传输态 | STAT、LIST、RETR、DELE、NOOP、RSET、QUIT、TOP、UIDL |
| 更新态 | QUIT |

### 5.2.4 PEM 标准安全问题

通过以上分析，SMTP 和 POP3 两项协议都存在着严重的安全漏洞。由 RFC1421、RFC1422、RFC1423 和 RFC1424 规定的 Internet 保密增强邮件标准 PEM 在邮件的保密安全性方面大大地强于 SMTP 和 POP3 协议。RFC1421 介绍了消息加密和验证过程，RFC1422 给出了基于证书的密钥管理，RFC1423 讲述了算法、模式和身份认证，RFC1424 讲述了密钥证书和相关服务。PEM 的最大特点是采用了公开密钥管理体制及基于这种体制的公开密钥证书机制。

#### 1. PEM 消息的格式

PEM 定义了四种格式的消息：ENCRYPTEN、MIC-ONLY、MIC-CLEAR 和 CRL。

ENCRYPTEN 消息具有可信性、真实性，提供 MIC 检查。

MIC-ONLY 比 ENCRYPTEN 消息缺少可信性，但仍然提供 MIC 检查和重编码。

MIC-CLEAR 消息比 MIC-ONLY 消息缺少重编码这一步，可用非 PEM 软件查看邮件内容。

CRL 消息用于传输注销证书列表之用，需要签名和重编码。

在设计和实现增强型保密电子邮件时，为了尽可能地提高电子邮件的安全性能，考虑到信息的保密性、真实性、完整性的实现，详细讨论了第一种和第二种 PEM 格式，因为第一种和第二种格式提供的安全性能较第三种和第四种强得多。

ENCRYPTEN 消息格式如表 5-3 所示；MIC-ONLY 消息格式如表 5-4 所示。

**表 5-3 ENCRYPTEN 消息格式**

| 域 | 含 义、内 容 |
|---|---|
| Pre-EB | “----BEGIN PRIVATE-ENHANCED MESSAGE----” |
| Proc-Type | 定义消息处理类型，此种格式只能为“4，ENCRYPTEN” |
| Content-Domain | 指明消息内容的表示方式，目前只有“RFC822”一种 |
| DEK-Info | 指明消息使用的加密算法和参数，目前算法标志只规定了“EDS-CBC” |
| Orgin-Cert | PEM 消息发送方证书 |

续表

| 域 | 含 义、内 容 |
| --- | --- |
| Key-Info | 定义密钥管理参数,包括 IK 算法标志和 IK 加密的 DEK。在此处的 Key-Info 是可选的 |
| Issuer-Cert | 发送方证书签发者证书 |
| MIC-Info | 消息集成校验信息 |
| Recpnt-ID-Asym | 接收方身份,包括接收方证书管理机构和版本/有效期 |
| Key-Info | 定义密钥管理参数,包括 IK 算法标志和 ID 加密的 DEK |
| PEM-Text | PEM 消息正文 |
| Post-EB | "----END PRIVACY-ENHAWCED MESSAGE----" |

表 5-4 MIC-ONLY 消息格式

| 域 | 含 义、内 容 |
| --- | --- |
| Pre-EB | "----BEGIN PRIVATE-ENHANCED MESSAGE----" |
| Proc-Type | 定义消息处理类型,此种格式只能为"4,MIC-ONLY" |
| Content-Domain | 指明消息内容的表示方式,目前只有"RFC822"一种 |
| Orgin-Cert | PEM 消息发送方证书 |
| Issuer-Cert | 发送方证书签发者证书 |
| MIC-Info | 消息集成校验信息 |
| PEM-Text | PEM 消息正文 |
| Post-EB | "----END PRIVACY-ENHAWCED MESSAGE----" |

### 2. PEM 消息加密和验证过程

PEM 使用两级密钥:数据加密密钥(DEK)和交换密钥(IK)。PGP 采用了单钥公开密钥管理体制,DEK 用来加密消息正文和计算消息集成校验(MIC),同时用来加密 MIC 的签名表示。DEK 一般每次会话生成一个,以达到"一次一密"的效果。而 IK 用来加密 DEK,以便在每次会话的初始段对 DEK 进行加密交换。加密 DEK 的 IK 就是发送方私钥,即实现对 MIC 的签名。依据 PEM 的机制,加密和签名过程的表达式如下:

```
Transmit-Form=Encode (Encrypt (Canonicalize (Local-Form)))
```

图 5-2 为 PEM 邮件加密签名生成的流程。

解密和验证过程的表达式为:

```
Local-Form=DeCanonicalize ((Decrypt (Decode (Transmit-form)))
```

图 5-3 为 PEM 邮件接收和验证的流程。

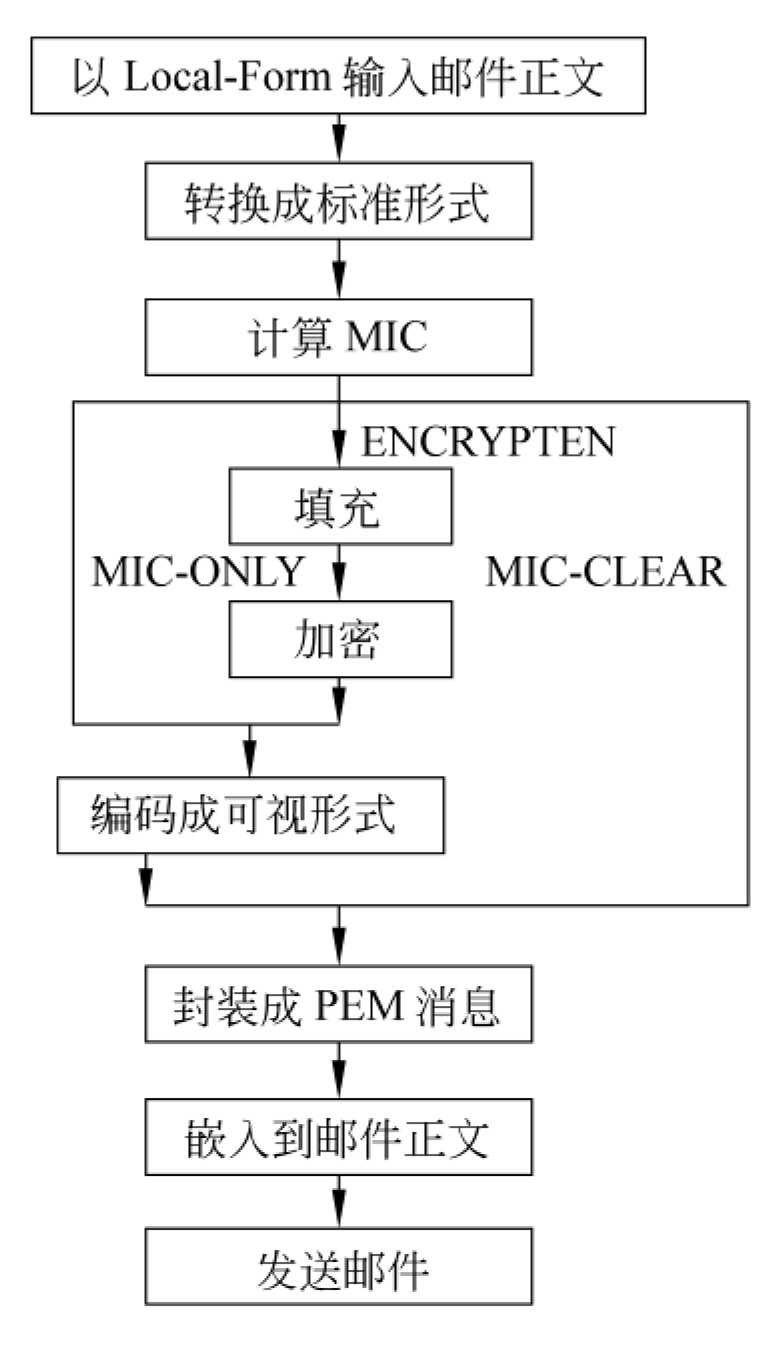





图 5-2 PEM 邮件加密签名生成过程

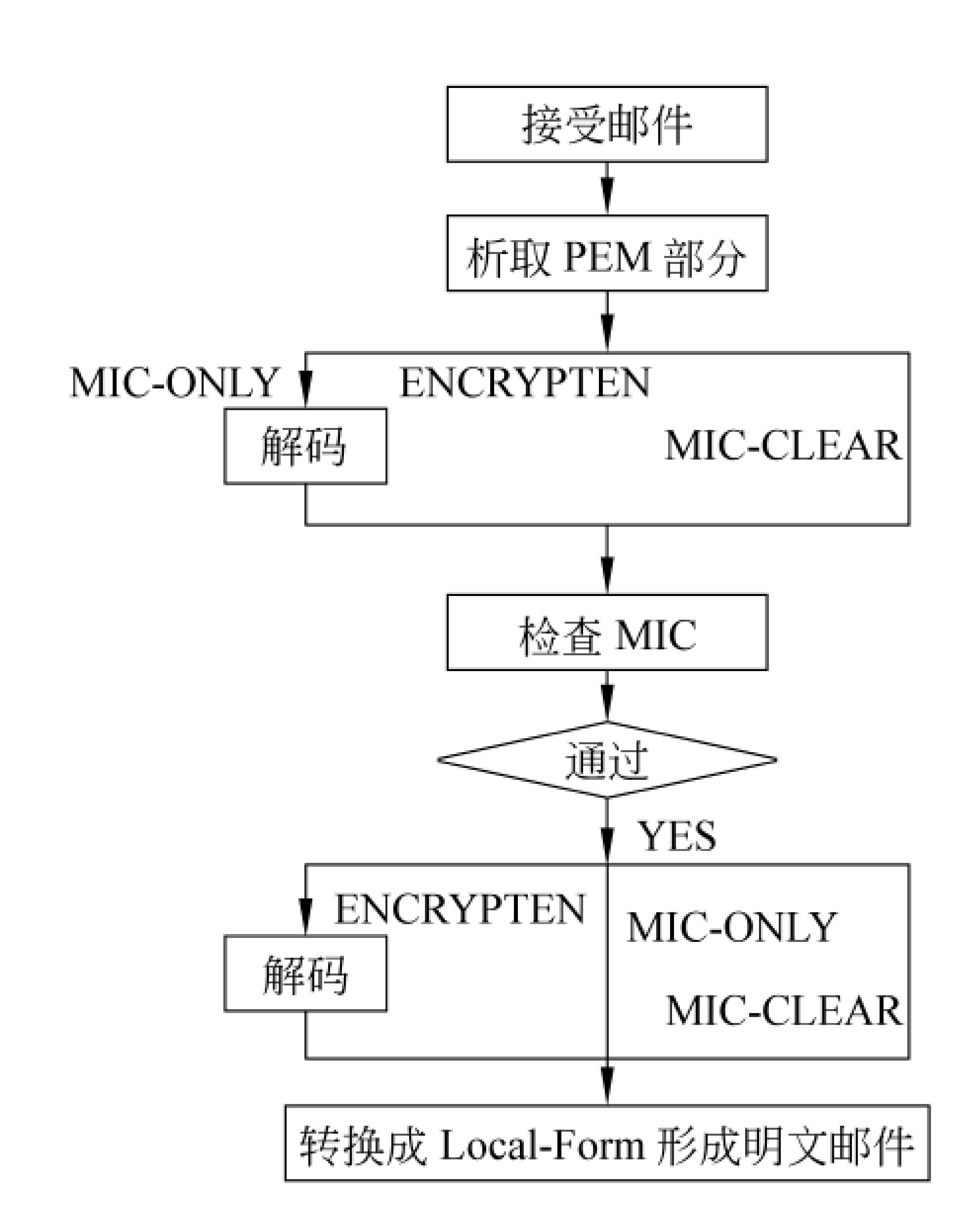



图 5-3 PEM 邮件接收和验证过程

### 3. PEM 密钥管理方式

PEM 与 PGP 的最大差别在于 PEM 采用了基于证书的密钥管理体制。证书是数字签名、身份认证、密钥管理等各种保密措施的综合运用，它提供的安全明显高于 PGP 等非证书密钥管理体制。

在密钥交换过程中存在着一个通信双方身份相互认证的过程，为了保护对方身份认证过程的正确性，应从可信的第三方获得对方的公钥等信息。这个可信的第三方就被称为证书中心(certification authority，CA)。证书中心应用公钥算法产生用户证书以保证用户身份的合法性。

证书中心通过对用户信息进行签名产生证书，证书内容包括用户名、用户公钥和一些附加信息。X. 509 标准对证书格式有详细的说明。一般说来，具体的用户证书信息由签发此证书的 CA 确定。在证书中心签发出用户证书后，证书就具有两个特性。

(1) 任何用户都可恢复出证书中隐藏的公钥，保证用户能得到证书中心的公钥。

(2) 证书是不可伪造的，只有证书中心可以更改证书。

假设用户名为 A，用户身份号为 UA，证书中心名为 CA，证书中心身份号为 UCA，则 CA 签发的证书如下：CA＜＜A＞＞＝CA{V，SN，AI，CA，UCA，A，UA，AP，TA}。其中，V 代表证书的版本号；SN 代表证书的系列号；AI 代表签发证书所用的加密算法；UCA 代表证书中心的身份号，可选；UA 代表用户的身份号，可选；AP 代表用户的公开密钥；TA 代表证书的有效期，包括一个证书有效起始时间和失效时间。PEM 使用的证书格式如表 5-5 所示。

表 5-5　PEM 证书格式

| 域 | 内　　容 |
|---|---|
| Version | 证书版本号,以便于证书格式的更新 |
| Serial Number | 证书序列号,具有唯一性 |
| Signature | 证书签发者的签名,包括签名算法和参数 |
| Issuer Name | 证书签发者的名称 |
| Validate Period | 证书有效期 |
| Subject Name | 证书持有者名称 |
| Subject Publickey | 证书持有者公钥 |

证书中心签发证书时,将涉及证书的申请、分发、存放以及注销、失效等一系列过程。这些过程,除了证书的申请,都可以通过网络自动进行。证书的存放需要维护证书库,所有未到期但又因怀疑有问题而注销的证书以及未到期而更换的旧证书须放入“黑名单库”,黑名单库对网络中的所有用户公开,以便于用户在解密邮件时核对对方证书的有效性。

由于地域的广阔性和用户的复杂性,使用单个 CA 管理所有用户是不可能的,因此,就必须对 CA 分级,实现密钥的分级管理。在 RFC1422 中规定证书的管理分 4 级,IPRA、PCA、CA 和用户或团体。IPRA 是 Internet 注册管理局,是在 Internet 内所有的证书的唯一的根。IPRA 的下一级是策略证书管理局(PCA),每个管理局负责为 CA、用户或机构注册。每个 PCA 由 IPRA 签发证书,在 PCA 的下一级设立证书管理局(CA),以签证用户和下属机构,大多数用户都会在这些机构中注册。但也有一些用户希望独立注册,这就需要另外的一些 PCA 为其签发证书。这样,这 4 级模式就形成了基于证书的密钥管理的分层结构。即使分为 4 层的证书管理在一些情况下对 CA 来说也是太过庞大,所以在实际应用中 CA 下面又可分出几层,以实现证书链的管理方式。图 5-4 所示即为一简单证书链。

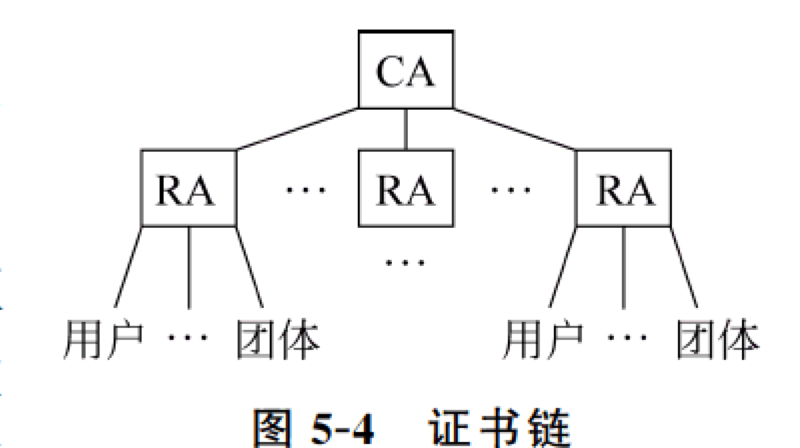



图 5-4　证书链

#### 4. PEM 工作原理

(1) A、B 分别向某个 CA 申请各自的证书。
(2) A 要向 B 发送邮件,必须先获得 B 的证书。
(3) A 获得为 B 签发证书的 CA 证书,验证该证书的有效性。
(4) 验证通过后,A 利用证书中的 B 的公钥,生成 PEM 邮件发送给 B。
(5) B 收到邮件后,要检查邮件的真实性,必须获得 A 的证书。
(6) B 为了验证 A 的证书的合法性,要获得 A 端 CA 的证书。
(7) B 验证 A 的证书合法后,解密 PEM 邮件。

#### 5. PEM 安全性分析

PEM 标准将各种安全技术综合于一体，其安全性几乎是无懈可击的。但是在密钥管理方面，虽然应用了基于证书的密钥管理，其中仍有一些小小的不足之处。在证书申请时，用户需将自己的公钥置于申请书中，形成申请证书报盘。但这时公钥不能加密，否则别的用户包括 CA 就会将加密的公钥当做公钥本身使用，使申请的证书无效或别的用户根本无法使用此证书。既然证书申请不能加密，如果在申请报盘时被第三者截获，用自己的公钥替代申请书中的公钥，而 CA 签发的证书由于 CA 无法察觉公钥的正确与否而被认为有效，那么以后所有发给证书申请者的邮件都可能被第三者截获并解密，PEM 就毫无安全性可言了。因此，在实际解决这个问题时，证书申请报盘不能通过网络自动运行，必须由用户按规定填写证书文件，生成公开密钥对，产生申请报盘，由人工送至 CA 处进行证书申请。

### 5.2.5 安全策略

#### 1. 对电子邮件进行加密

既然没有任何办法可以阻止攻击者截获在网络上传输的数据包，那么，唯一能采取的措施就是在发送邮件前对其进行数字加密处理，接收方接到电子邮件后对其进行数字解密处理。这样，即使攻击者截获了电子邮件，他面对的也只是一堆没有任何意义的乱码。加密，是指将一个明文信息经过加密密钥及加密函数的转换，变成无意义的密文，当需要的时候则将此密文经过解密函数、解密密钥还原成明文。最常用的加密软件是 PGP (pretty good pri-vacy)。PGP 是一个基于 RSA(rivest shamir adleman)公钥加密体系的邮件加密软件，它提出了公共钥匙或不对称文件加密和数字签名。RSA 算法是一种基于大数不可能质因数分解假设的公钥体系。简单地说，就是找两个很大的质数，一个公开给世界，称为“公钥”，另一个不告诉任何人，称为“私钥”。两把密钥互补——用公钥加密的密文可以用私钥解密，反过来也一样。假设 A 寄信给 B，他们知道对方的公钥，A 可以用 B 的公钥加密邮件寄出，B 收到后用自己的私钥解出 A 的原文。这样就保证了邮件的安全，以防止非授权者阅读，还能对邮件进行数字签名从而使 B 确信邮件是由 A 发出的。

#### 2. 对邮件和系统进行病毒防护

1）选择一款可靠的防毒软件

目前常用的防毒软件有瑞星、KV3000、KILL、金山毒霸、诺顿等，用户可打开防毒软件的电子邮件扫描功能，对来往邮件的病毒进行拦截，可有效防止邮件病毒的侵入，并防止将感染病毒的电子邮件发送给其他用户。

2）及时升级病毒库

计算机病毒在不断产生并演化变体，反病毒软件生产商都会根据最近新发现的病毒情况，随时补充新病毒代码到病毒库中，因此，及时升级防病毒软件是必须做的工作。

3）识别邮件病毒

一些邮件病毒具有广泛的共同特征，找出它们的共同点可以防止病毒的破坏。当收到邮件时，先看邮件大小及对方地址，如果发现邮件中无内容、无附件、邮件自身的大小又有几十 K 或更大、附件的后缀名是双后缀等，那么此类邮件中极可能包含有病毒，可直接删除此邮件，然后再清空废件箱。在清空废件箱后，一定要搜索一遍邮箱；否则杀毒软件在下次查毒时还会报病毒。

4）打开实时监控防火墙

实时监控技术为电子邮件和系统安全构筑起一道动态、实时的反病毒防线，它通过修改操作系统，使操作系统本身具备反病毒功能，拒病毒于计算机系统之门外。优秀的反病毒软件由于采用与操作系统的底层无缝连接技术，实时监控器占用的系统资源极小，用户几乎感觉不到其对机器性能的影响，并且不用考虑病毒的入侵问题。

5）投石问路

当遇到带有附件的邮件时，如果附件为可执行文件（*.exe、*.com）或带有宏功能的 Word 文档时，不要选择打开，可以用两种方法来检测是否带有病毒。一种是利用杀毒软件的邮件病毒监视功能来过滤邮件中的病毒；另一种是把附件先另存在硬盘上，然后利用杀毒软件进行查毒。

6）尽量不在“地址簿”中设置联系名单

因为一旦被病毒感染，病毒会通过邮件“地址簿”中联系人的邮箱来传播。

7）少使用信纸模块

信纸模块往往是一些脚本文件，如果模块感染了脚本病毒，如欢乐时光、VBS/KJ 等，那么用户使用信纸发出去的邮件就带有病毒了。

8）设置邮箱自动过滤功能

通过 Web 上网收发邮件的用户可以把陌生的邮件人地址列入自动过滤，以后就不会再有相同地址的邮件出现了。这样不仅能够防止垃圾邮件，还可以过滤掉一些带病毒邮件，使其不进入收件箱中，减少病毒感染的机会。

9）不使用邮件软件中的预览功能

目前，一些感染性、破坏力较强的病毒往往是不需要打开邮件通过邮件预览时进行感染。如果使用 outlook 收发邮件，建议用户关掉邮箱工具的预览项或者升级微软的最新补丁，以预防 outlook 接收邮件时被感染。如果使用的是 foxmail，在当前账户属性中模块项选择纯文本格式。

### 3. 垃圾邮件和邮件炸弹的防范措施

（1）不要随便公开自己的信箱地址，尤其是 ISP 信箱。即使要公开也得做些技术加工，比如 Bill#163.net 或以图片代替，加了这类符号可逃过专业邮寄地址分离器的搜索，而对方也看得懂。如因工作需要，既要使用对外公开的邮箱，又要经常发送一些相对保密的邮件最好使用两个甚至两个以上的邮箱，用不同的邮箱联系不同的人，这样即使受到攻击也不会造成过多的损失。

（2）对付垃圾邮件最好使用垃圾邮件清除软件进行过滤、自动删除，它们可以为用户

提供方便而强大的保护。常用的有 Spamkiller（垃圾邮件杀手）、SpamEater Pro（垃圾邮件吞食者）、Spam Attack Pro（垃圾邮件终结者）等。也可使用 BombCleaner 等炸弹清理软件，在不接收信件的时候查看邮件清单，从中选择垃圾信件进行远程删除，这样既节约了大量下载信件的时间，又堵住了通过电子邮件传播的病毒。

(3) 用户在设置“过滤”时，要注意“接收信件大小”选项，一般将这个数值控制在电子信箱容量的 1/3 左右。如果发过来的信件大小超过了这个数值，就被认为是邮件炸弹而直接被系统舍弃，这样邮件炸弹就毫无威胁可言。

(4) 电子邮件的过滤器可使用户按照邮件的来源、主题、长度、接收者来设置过滤规则。过滤器可设置在本地的电子邮件客户端程序上，也可通过浏览器在 POP3 信箱的内部进行设置。前者是在接收电子邮件的时候对邮件是否属于垃圾或炸弹进行判断，其缺点是在信箱被塞满的时候失效。后者是通过浏览器登录到 POP3 服务器上，进入自己的信箱，找到“邮件收发设置”，并且在其中的过滤器内填写有关发送垃圾邮件的邮件地址，确认保存后就能在服务器上过滤掉垃圾邮件和炸弹邮件，确保信箱的安全。

#### 4. 采用防火墙技术

防火墙是在受保护的内部网和外部网之间建立的网络通信安全监控系统，也可称为控制进/出两个方向通信的门槛。在网络边界上通过建立起来的相应网络通信监控系统来隔离内部和外部网络，以阻挡外部网络的侵入。目前的防火墙主要有包过滤防火墙、代理防火墙和双穴主机防火墙 3 种类型。其中应用最广泛的防火墙为代理防火墙又称应用层网关级防火墙，它是由代理服务器和过滤路由器组成。过滤路由器负责网络互联，并对数据进行严格选择，然后将筛选过的数据传送给代理服务器。代理服务器起到外部网络申请访问内部网络的中间转接作用，其功能类似于一个数据转发器，它主要控制哪些用户能访问哪些服务类型。当外部网络向内部网络申请某种网络服务时，代理服务器接受申请，然后它根据其服务类型、服务内容、被服务的对象、服务者申请的时间、申请者的域名范围等来决定是否接受此项服务。如果接受，它就向内部网络转发这项请求，从而保护了内部网络不被非法访问。

基于以上分析，可以看出利用防火墙可以加强邮件的安全性。合理配制防火墙可以限制邮件的访问，使之只发送到有限的几个机器上。加强对这些机器的防范，可将这些机器作为进入内部网络的网关来控制邮件的出入，因此，用防火墙来对付邮件炸弹的轰炸是非常有益的。合理设置防火墙可确保所有外部的 SMTP 联接到一个邮件服务器上，这样会有一个集中的登录地点，便于追踪不正常的邮件。

## 5.3 Web 安全策略

随着网络应用之间通信和互操作的增多，基于 Web 服务的应用也在快速发展。Web 服务是一种完全建立在现有互联网标准之上、松散耦合的、跨语言和平台的应用程序之间通信的标准方法。Web 服务及其安全性的研究正受到人们日益广泛的关注。

在分布式网络环境中，全面的安全 Web 服务依赖于每一个参与的系统，以及它们之

间的协同工作。Web 服务的基础是简单对象访问协议 SOAP，它是在分布式环境中交换信息的简单的 XML 文本协议，因为本身具有安全隐患，从而也就决定了 Web 服务本身存在一定的安全问题。一般而言，信息传输的安全要求有以下几点：保密性，保证没有经过授权的用户、实体或进程无法窃取信息；授权，确定允许用户做什么的过程；数据完整性，信息在传送的过程中保持完整和统一；信息源认证，对信息或数据的发送者进行的标识；不可否认性，保证信息的发送者不能否认对信息的发送。

### 5.3.1 WWW 面临的安全威胁

WWW 应用由 3 个部分构成：提供 WWW 服务的 WWW 服务器、使用 WWW 服务的 WWW 浏览器以及传递浏览器和服务器之间服务请求和响应报文的网络。这 3 个部分都面临安全的威胁。

从服务器角度看，WWW 服务器通常作为某个机构向外发布信息的一个公共信息服务的窗口，它应该允许任何用户访问 WWW 服务器。而根据网络安全的要求，安全的网络服务器必须对用户进行身份验证，不能允许匿名者访问。这样，WWW 提供的服务本身就与网络安全要求相互矛盾。

万维网服务器安全漏洞主要源于两个方面：一是 WWW 服务器软件错误而产生的安全漏洞；二是 WWW 服务器配置不当而产生的安全漏洞。这些安全漏洞都会允许远地网络用户非法进入 WWW 服务器，窃取其中非公开的数据和文件，执行非授权的修改系统的命令，发起“拒绝服务”攻击，使 WWW 服务器处于“不可用”状态。

WWW 服务器上的安全漏洞在某种程度上是不可弥补的，因为根据目前的软件技术水平，复杂而庞大的软件系统一定会有软件错误。而 WWW 应用就是一个复杂而庞大的软件系统，确实已经发现了不少软件错误。复杂而庞大的软件系统配置也相应比较复杂，很容易发生配置错误。

在这种软件错误和人为配置错误存在的情况下，对 WWW 服务器进行安全保护，是一项目前尚未成熟的技术，只能通过一些技巧处理。例如，通过一些受控的网络攻击软件，自动进行“受控”网络攻击，检测 WWW 服务器的安全漏洞。这里的关键是“受控”攻击，否则会产生截然相反的效果。另外，也可以及时浏览安全预警网站，及时获得有关软件错误的信息，及时更新软件版本。

从浏览器角度看，WWW 浏览器的作用就是在公共互联网上发现感兴趣的 WWW 网站，浏览并且下载这些 WWW 服务器上有价值的信息。但是，由于现在浏览器都支持 Java 语言和 Java 脚本这类移动代码编制的动态内容，这些内容可以在浏览器上运行。如果这些动态内容中嵌入恶意代码，则会破坏浏览器、损伤浏览器所在的计算机系统、窃取浏览器所在的计算机系统中用户的敏感数据等。从浏览器角度防范恶意代码，这既属于一类蠕虫防范问题，也属于 WWW 安全问题。这类客户端系统防范网络攻击问题是目前比较困难的安全问题。

从网络角度看，主要的安全危险来自于对 WWW 浏览器和服务器之间传递数据的窃听、篡改、假冒和重播报文攻击，这也是网络安全主要研究的问题。这方面目前已有比较有效的安全技术，例如，前面章节介绍的传送层安全技术中的安全套接层（SSL）技术就是

针对 WWW 浏览器和服务器之间保密、完整地进行数据交互而设计的。

### 5.3.2 WWW 安全防范技术

根据以上对 WWW 应用环境下安全威胁的分析，可以将 WWW 的安全防范技术分成 3 个域：浏览器安全防范域、网络安全防范域以及服务器安全防范域。需要说明的是，进行 WWW 的安全防范实际上就是保证 WWW 服务的保密性、完整性和可用性。

从目前的网络安全技术看，保证 WWW 服务的保密性和完整性技术比较成熟。可以采用在前面章节介绍的传送层安全技术中的安全套接层(SSL)技术，在 WWW 浏览器和服务器之间建立一条 SSL 秘密通道，所有在浏览器和服务器之间传递的报文都经过加密和签名之后才在网络环境下传递。这样，如果浏览器用户保管好自己的私钥，就可以防范网络攻击者对 WWW 浏览器和服务器之间传递数据的窃听、篡改、假冒和重播报文攻击。

但是，目前的网络安全技术尚不能保证 WWW 服务器、浏览器和网络的可用性，即目前还无法完全防范“拒绝服务”类的网络攻击以及探测系统漏洞进行“网络蠕虫”攻击的网络威胁。实际上，目前对网络最大的安全威胁就来自于分布式“拒绝服务”攻击以及“网络蠕虫”攻击。

当然，目前也设计了一些保护 WWW 浏览器和服务器可用性的技术，例如，在公共 WWW 服务器前端设置一个 WWW 服务器防火墙，用于过滤异常的 WWW 服务请求，保护 WWW 服务器不受“拒绝服务”这类攻击。这种 WWW 防火墙是专门针对 WWW 服务器设计的一个访问控制系统，它本身携带安全策略库和审核数据库，用于控制进出 WWW 服务器的报文。它比一般的网络防火墙针对性强，可以制定较为详细的、有针对性的安全控制策略，并且可以通过及时调整安全控制策略，防范潜在的网络攻击。

在浏览器上也设计了类似专用防火墙的技术，用于过滤进入浏览器的数据，包括 Java 语言和 Java 脚本编制的动态代码，通过特征分析剔除可能的恶意代码。

### 5.3.3 Windows IIS 安全设置

#### 1. 安全性

(1) 摘要式身份验证在使用 HTTP 端口的情况下，提供了可靠的安全性。由于使用 HTTP 端口，摘要式身份验证允许跨代理服务器和防火墙对用户进行安全和严格的身份验证。另外，还可进行匿名、HTTP 以及集成 Windows 身份验证。

(2) 安全套接字协议层(SSL) 3.0 和传输协议层安全(TLS)提供了一种客户端与服务器之间进行信息交换的安全方式。另外，SSL 3.0 和 TLS 还为服务器提供了一种在用户登录服务器之前对客户端进行验证的方法。在 IIS 5.0 中，ISAPI 和 Active Server Pages 都可以访问客户证书，以便编程人员通过其站点跟踪用户。同时，IIS 5.0 还可以将客户证书映射为 Windows 账户，以便管理员可以根据客户证书控制对系统资源的访问。

(3) 服务器网关加密(SGC)是 SSL 的扩展，允许使用 IIS 出口版的金融系统采取加密性能更高的 128 位加密。虽然 IIS 5.0 中已内置了 SGC 功能，但使用 SGC 时仍然需要特殊的 SGC 证书。

(4)“Web 服务器证书向导”简化了证书管理任务,如创建证书请求以及管理证书生存期。“权限向导”通过向虚拟目录和文件分配访问策略的方式,从而简化了配置 Web 站点访问的任务。“权限向导”还可以更新 NTFS 文件权限来反映 Web 访问策略。“CTL 向导”可帮助配置证书信任列表(CTL)。CTL 是特定目录的可信证书颁发机构列表(CA)。CTL 对于那些在服务器上有同一个 Web 站点,并且要求每个站点拥有不同可信证书颁发机构列表的 Internet 服务提供商(ISP)尤其有用。

(5) IP 地址及 Internet 域限制,可以授予或拒绝单台计算机、计算机组或整个域对 Web 的访问。

(6) Kerberos 5 身份验证协议相容性,IIS 已完全集成了 Windows 2000 中实现的 Kerberos 5 验证协议,从而允许用户在运行 Windows 的计算机之间传递验证凭据。

(7) IIS 证书存储目前已与 Windows CryptoAPI 存储集成在一起。Windows Certificate Manager 提供单一入口,允许用户存储、备份和配置服务器证书。

## 2. 可管理性

(1) 重新启动 IIS。现在不用重新启动计算机就可以重新启动 IIS 服务。

(2) 备份和还原 IIS。可以备份和存储 metabase 设置,以便更容易返回已知的安全状态。

(3) 进程账户。提供关于单个 Web 站点如何使用服务器中 CPU 资源的信息。此信息在判断哪些站点正在不成比例地使用 CPU 资源或者具有不正常的脚本和 CGI 进程时非常有用。

(4) 进程限制。可以限制 CPU 在处理单个 Web 站点的进程外 ASP、ISAPI 以及 CGI 应用程序的时间百分比。另外,还可以终止和重新启动行动失常的进程。

(5) 改进的自定义错误消息。当 Web 站点出现 HTTP 错误时,管理员可以向用户发送消息。同时,通过使用 500-100.asp 自定义错误消息,还可以包含详细的 ASP 错误进程功能。可以使用 IIS 5.0 提供的自定义错误消息,也可自定义错误消息。

(6) 配置选项。可以在站点、目录或文件级别设置“读取”、“写入”、“执行”、“脚本”,以及“FrontPage Web”操作的权限。

(7) 远程管理。IIS 5.0 已经包含一些基于 Web 的管理工具,可以从任何平台的几乎所有浏览器上远程管理服务器。利用 IIS 5.0,可以设置称为操作员的管理账户,使之具备一定的 Web 站点管理权限,帮助分担一部分管理任务。

(8) 终端服务。终端服务属于 Windows 2000 的一种功能,允许用户在终端以及在个人计算机和其他计算机桌面上运行的终端模拟程序上运行 32 位的 Windows 应用程序。终端服务事实上允许任何桌面运行服务器上的应用程序,这样就可以远程管理 IIS 等 Windows 2000 服务,包括从旧的 PC,甚至从非 PC 设备进行管理,用户好像就在服务器控制台前一样。

(9) 集中管理。IIS 使用 Microsoft Management Console(MMC)时的管理工具。MMC 支持管理员用于管理服务器的程序,称为管理单元。可以从运行 Windows 2000 Professional 的计算机上使用 IIS 管理单元,管理运行有 Internet 信息服务的 Windows

2000 Server 计算机。

### 3. 可编程性

Active Server Pages(ASP)可以使用服务器端的脚本和组件创建动态内容,从而创建与浏览器无关的动态内容。由于 ASP 允许开发者将任何脚本语言或服务器组件嵌入 HTML 页中,从而提供了一种 CGI 和 ISAPI 的简便方法。ASP 提供对所有 HTTP 请求和应答流的访问,以及对标准数据库链接的访问,同时还允许自定义适合各种不同浏览器的内容。

ASP 新增和改进了一些功能,这样有助于改善性能以及简化服务器端的脚本。

IIS 5.0 为 Web 应用程序提供更大的保护以及更强的可靠性。默认情况下,IIS 在公共或"公用"进程(即与核心 IIS 进程隔离的进程)中运行应用程序。而且还可以隔离执行关键任务的应用程序,这些程序应该在核心 IIS 以及共用进程之外运行。

在 IIS 5.0 中,管理员和应用程序开发者可以向现有的 ADSI 提供者添加自定义对象、属性和方法,从而进一步增大了管理员配置站点的灵活性。

### 4. 信息发布

IIS 5.0 版符合 HTTP 1.1 标准,包括 PUT 和 DELETE 等功能以及自定义 HTTP 错误消息的能力,并支持自定义的 HTTP 头。

由于支持主机头,解决了多个域名对应一个 IP 地址的情况,因此可以用一个 IP 地址在运行 Windows 2000 Server 的单台计算机上维护多个 Web 站点。这对于 Internet 服务提供商以及维护多个站点的 Intranet 非常有用。

允许远程用户通过 HTTP 连接创建、移动或删除服务器上的文件、文件属性、目录和目录属性。

可以使用 SMTP 服务以及 NNTP 服务设置与 IIS 一同工作的 Intranet 邮件和新闻服务。

可以将 Platform for Internet Content Selection (PICS)分级应用于内容仅适合于成人的站点。

如果在数据传输中出现中断,现在可以恢复"文件传输协议"文件下载,而不必再次下载整个文件。

可以更快地在 Web 服务器与启用了压缩的客户之间进行页面传输。压缩和缓存静态文件并对动态生成的文件按需进行压缩。

### 5. 虚拟服务器与虚拟目录

可以在一台服务器上安装多个 Web 网站,使用时就好像这些网站分别处于不同的计算机一样。这种服务器称为虚拟服务器。

配置虚拟服务器的方法主要有 3 种。

(1) IP 法。通过多个网卡或者一个网卡绑定多个 IP 地址的方法实现。

(2) 端口法。在同一个 IP 下通过分配不同的端口号来实现,IIS 中的远程管理就是

这样实现的,使用的端口范围为 1024～65 535。

(3) 主机头法。在 HTTP 1.1 协议版本的基础上,使用同一个 IP 及同一个端口的前提下,通过完全域名实现虚拟主机,是最实用的方法。注意,需要在 DNS 或者客户端的 host 的文件中作解析,而且客户端的浏览器要支持 HTTP 1.1 协议。

通过 Web 站点创建向导,使用主机头法创建虚拟服务器,如图 5-5 所示。

Web 站点创建向导
IP 地址和端口设置
为新 Web 站点指定 IP 地址和端口设置。
输入 Web 站点使用的 IP 地址(E):
127.0.0.1
此 Web 站点应使用到的TCP 端口(默认:80)(T):
80
此站点的主机头(默认:无)(H):
www.xl1.edu.cn
此 Web 站点应使用的 SSL 端口(默认:443)(L):
若要获取更多的信息,请参阅 IIS 文档。
< 上一步(B) 下一步(N) > 取消

图 5-5　主机头法创建虚拟服务器

也可以通过修改 Web 站点属性来添加虚拟服务器,如图 5-6 所示。




图 5-6　Web 站点属性添加虚拟服务器

在创建网站时都需要定义一个主目录,作为存放网站信息文件的主要场所。主目录下的实际子目录当然也可以存放网站文件,但也可以定义一些不相关的目录,使其好像是在主目录下,与目录下的子目录一样存放网站文件。这些目录叫做虚拟目录。虚拟目录可以在本地的其他分区上,还可以在网络中的其他服务器上。

比如微软站点的服务器在美国,而微软中国站网址是 http://www.microsoft.com/china,这个"china"就是虚拟目录的别名,其实这个服务器的物理位置在中国,但逻辑上它作为微软站点的一个子目录。

创建虚拟目录有以下几种方法。

(1) 使用本地主机的目录。

(2) 使用另一主机的网络共享目录,需要提供一个有效的用户名及密码。

(3) 重定向到 URL。

Web 站点的管理依赖于站点属性的配置,这些配置是在属性表单中进行的。IIS 管理控制树中的任何节点都拥有自己的属性表单,如计算机、站点、虚拟目录、文件等,可以在属性表单中分别配置其属性。右击 IIS 管理控制树的相应节点,在弹出的快捷菜单上选择"属性"项,就可以打开属性表单。IIS 定义一套属性继承机制,即低层子属性自动继承高层父属性。例如,若更改计算机属性表单使计算机属性与当前的某个站点属性有所

冲突，那么，基于属性继承的原则，冲突的站点属性被动继承计算机属性。这里，计算机属性表单又称为主属性表单。

在IIS管理控制树中右击计算机图标，在弹出的快捷菜单中选择“属性”菜单，打开计算机属性对话框，其中有两个选项卡。在“Internet信息服务”选项卡中，可以分别配置WWW服务和FTP服务的主属性、计算机的总带宽截流、邮件发送方式、系统权限等属性。对任一属性进行更改后，单击“应用”按钮，再单击“确定”按钮使之生效。

Web站点属性表单是配置Web站点属性的主要界面，在IIS管理控制树中右击Web站点节点，在弹出的快捷菜单中选择“属性”菜单，打开Web站点属性对话框。默认Web站点的属性表单由10个选项卡组成，可以分别对Web站点各个方面的属性进行配置。下面就是一些重要属性。

(1) 主目录就是用于存储站点相关文件的主要路径，包含着站点文件的其他目录或是直接位于主目录之下，或是以虚拟目录的形式挂在主目录下。在Web站点属性表单中单击“主目录”选项卡。在该选项卡中能够对站点主目录、文件及应用程序权限进行设置。

主目录的分配有3种方式：默认情况下选中“此计算机上的目录”选项，输入或单击“浏览”按钮指定本地主目录路径；选择“另一计算机上的目录”选项，可以指定远程主目录，具体形式是网络中共享文件夹的UNC路径“\\服务器名\共享名”；另一种指定主目录的方式是将主目录重新定向到一个URL，也就是Internet中的某个其他网站或其之下的目录，应选择“重定向URL”，并在“重定向到”栏输入URL地址。例如，输入Http://www.microsoft.com/china，即将Http://www.microsoft.com网站的/china目录作为当前Web站点的目录。

(2) 默认主页指用户在请求站点(例如，在浏览器地址栏中输入站点域名)后所收到的默认网页。通常也将网站的首页称为主页。一般情况下默认主页存储在主目录下，如index.htm或default.asp等。当然也可以改用其他的主页作为默认主页。其设置对话框如图5-7所示。

可以添加多于一个默认主页，所有添加的文档都显示在列表框中，选择一个文档，单击上下箭头调整其显示的优先级。通常会首先尝试加载优先级最高的主页，一旦不能成功下载，将降低优先级继续尝试。文档在列表中的位置越靠上意味着其优先级越高。

“文档”选项卡中不仅能够指定默认主页，还能配置文档页脚。文档页脚，又称footer，是一种特殊的HTML文件，用于使网站中全部的网页上都出现相同的标记，通常使用文档页脚将公司徽标添加到其网站中全部网页的下部，以增加网站的一致性。

为了使用文档页脚，首先勾选“文档”选项卡中的“启用文档页脚”复选框，然后单击“浏览”按钮指定页脚文件。页脚文件通常是一个.htm格式的文件。

(3) 通常网站会为自己的用户提供出错信息。HTTP协议提供了一系列标准的错误代码，分别指示出错原因以及错误对象、可能的处理方法等信息。例如，“404错误”代表客户机请求的文件不存在，“401.2错误”代表客户没有相应权限访问指定资源。

也可以重新编辑这些提示信息，使它们对客户更加有用，而不是对着一大堆术语束手无策。这样，就要先编辑一些包含针对各类错误进行提示的信息文件，然后将它们分




图 5-7　默认主页设置对话框

别映射到相应的 HTTP 错误类型上。

自定义错误信息的方法如下。

在 WWW 属性表单中单击“自定义错误信息”选项卡,列表中列出各种 HTTP 错误类型。

选择需要自定义的错误类型,单击“编辑属性”按钮。在“映射错误属性”对话框中配置自定义错误代码,如图 5-8 所示。

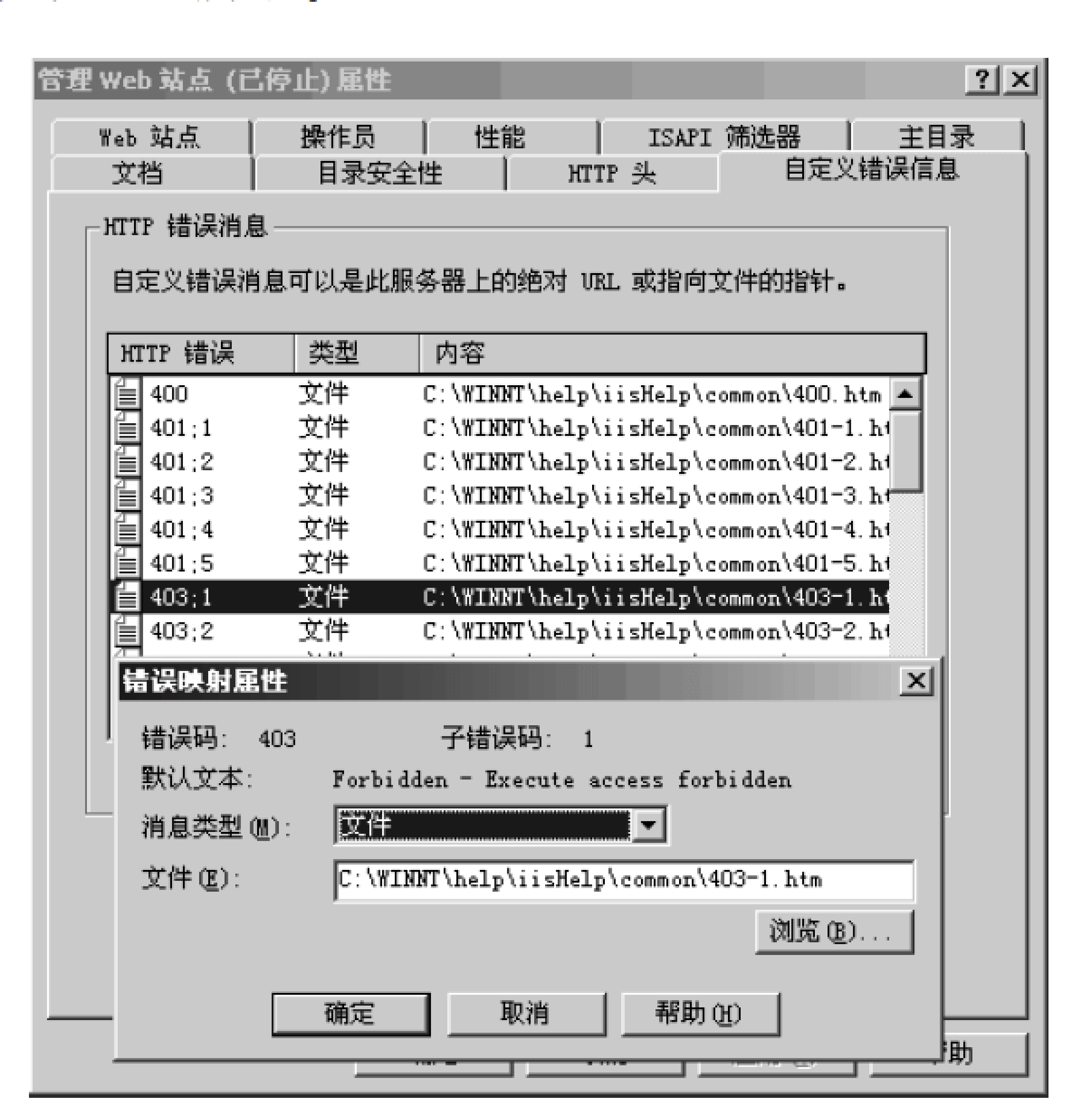



图 5-8　自定义错误信息对话框

(4) 在“Web 站点”选项卡中部的“连接”区域中，可以设置站点的连接属性，这些属性通常决定了站点的访问性能。由于硬件性能和带宽的限制，一个 Web 站点所允许的同时访问用户数量是有限的，过多的同时连接数往往可能导致种种问题，甚至网站当机。所以，对于访问数量大的站点而言，应限制同时连接数(默认情况下是不限制的)。单击“限制”按钮指定同时连接的数量即可。基于同样的原因，还应限制连接超时，连接超时是指一个连接到 Web 站点上的客户在一定的时间内如果没有做出任何响应，就将被自动断开连接。例如默认的连接超时为 900 秒，这意味着当一个当前连接客户连续发呆 15 分钟后将被自动剔出系统(即断开连接)，这样能有效地保护系统的资源。另外，“启用保持 HTTP 激活”复选框通常能够加快网站对用户的响应速度，该选项允许客户保持与服务器的开放连接，而不是使用新请求逐个重新打开客户连接。

(5) 调整 Web 站点性能，一般而言，在同样硬件配置条件下，不可能凭空提高系统的性能，所以，性能的调整实质上就是系统各部分之间的资源分配问题。例如，对于专用的 Web 服务器，显然应该尽量地将全部性能潜力都分配给 WWW 服务。而对于个别还需担当其他任务的计算机而言，则要在各种任务之间找到平衡点。

选择 WWW 属性对话框中的“性能”选项卡，其上部的性能调整滑块可以调整系统描述站点的大致访问量(每日期望单击数)，这一设定不具强制性，仅是为系统对资源的分配做出建议以供参考。为了限制当前站点占用的总带宽数量，可以进行带宽截流设置。选择“启用带宽限制”复选框，在“最大网络使用”栏中指定当前网站最多能够占用的带宽数，默认为 1024KB/s，达到这一限制时，多出部分的请求将被拒绝。上述限制多作用于网络资源，对于计算机本地资源，如 CPU 占用等，也有必要加以限制。选择“启用进程限制”复选框，在“最大 CPU 使用程序”栏中指定当前网站能够占用的最大 CPU 使用率，默认为 10%。这一限制并非强制性的，也就是说，即使达到最高 CPU 占用率，系统也并不会终止当前站点的运行，而只是适当降低其 CPU 占用率。如果需要在达到最大限制时强制性结束网站应用程序或其他进程，则需要勾选“强执行限制”复选框。注意，这一设置有可能带来系统稳定性上的问题。

(6) 日志是以文件形式监视网站使用情况的手段。“Web 站点”选项卡的下部是用于配置日志记录的区域，选择“启用日志记录”复选框，然后在“活动日志类型”下拉列表框中指定日志类型，各种日志类型的内在差别并不是很大，常用的日志类型有 W3C 扩展日志文件格式和 Microsoft IIS 日志文件格式。

选定日志文件类型后，单击“属性”按钮，打开“扩充日志记录属性”对话框。“常规属性”选项卡提供了一般性的日志文件设置界面。可以在“日志文件目录”栏中更改日志文件存储的路径。日志是一种持续性的记录手段，随着时间的推移，单个日志文件所记录的事件越来越多，其文件也越来越大。为了防止日志文件太大所导致的存储及分析困难，应该在日志文件达到一定大小时新建一个文件。通常的判断方法有两种，一定时间后新建文件和达到一定大小后新建文件。对于前者，只需选“每小时”、“每天”、“每周”或“每月”即可在指定时间到达时自动生成新的日志文件，新文件将以时间命名，例如，yymmdd.log 或 mmdd.log。然而当选择“当文件大小达到”并指定大小后，系统就可以在日志文件达到指定大小后自动生成新文件。

**注意**：记录过多的不必要内容必定会耗费有限的服务器资源，而且会使日志文件变得很大，因此，应确保所记录的事件都是必要的。

日志的保存方法及保存内容如前所述，但是这里记录的日志文件如何才能变成对于Web 管理员有用的信息呢？直接查看日志文件显然是方法之一，但要理解各种复杂的日志格式，并从中得到有用信息显然不是人力所能及之事。事实上，需要借助于其他工具完成日志文件的分析工作，例如，著名的 Microsoft Site Server 就是一种流行的日志分析工具。通过引入、分析日志文件，Site Server 最终给出一个便于理解的分析报告，报告以图形、图表等方式直观地显示出运行期间的各种事件。大多数的日志分析软件还能够设置过滤器，以便对管理员感兴趣的事件进行单独分析。

(7) 主目录选项卡还允许对站点文件和应用程序权限进行配置。对于文件，基本的权限有读取和写入，可分别勾选“读取”和“写入”复选框进行指定。其中，前者对于通常的静态网页站点是必需的，后者则允许客户对网站文件进行修改或添加。如果网站中包含脚本文件，则还应指定“脚本资源访问”权限。此外，还有一种特殊的权限——“目录浏览”。一旦指定目录浏览权限，即使客户没有读取权限，也能够查看网站的组织结构，看到网站中究竟有哪些文件，分别在什么位置。所以，指定该权限往往会带来安全性上的隐患。对于应用程序而言，权限有“纯脚本”以及“脚本和可执行程序”两种。它们是在“执行许可”下拉列表框中进行指定的。其中后一种权限包含前一种。所谓可执行程序与脚本程序的区别在于：可执行程序在服务器端执行，其通常的后缀为.exe、.bin、.dll、.com、.dat 等；而脚本程序是先下载到客户机，再解释执行的，它们采用脚本语言编写，如Vb Script、JSP、Perl、PHP 等。可选择的运行应用程序的保护方式有三种：与 Web 服务在同一进程中运行(低)、与其他应用程序在独立的共同进程中运行(中)，或者在与其他进程不同的独立进程中运行(高)。

(8) 在通常情况下，网站是允许匿名访问的，即无须输入账号，自动使用匿名访问账号并继承匿名访问权限。在安装 IIS 时，系统自动生成一个匿名访问用户账号 IUSR_computername，其中 computername 是 IIS 所在服务器的计算机名。所有 IUSR_computername 账号能够访问的资源，就是匿名用户的授权许可范围。

一旦用户所访问的资源不允许匿名访问，IIS 就会要求用户提供合法的用户账号及密码，这就是授权访问。授权访问要求用户拥有合法的 Windows 2000 账号，且必须具有相应的权限。

匿名和授权访问控制是在站点 WWW 属性对话框的“目录安全性”选项卡中进行的。默认情况下，IIS 对任意站点都是允许匿名访问的，如果出于站点安全性考虑需要禁止匿名访问时，按照如下步骤进行配置。

① 在 IIS 中右击管理控制树中需要禁止匿名访问的 Web 站点图标，选择“属性”菜单。

② 单击“目录安全性”选项卡。

③ 在“目录安全性”选项卡上部的“匿名访问和验证控制”栏中单击“编辑”按钮。

④ 在“验证方法”对话框中清除“匿名访问”复选框。

⑤ 单击“确定”按钮返回。

当然，对于公共性质的网站而言，并不需要禁止匿名访问，但是某些情况下还需要对匿名访问用户账号进行配置。在“验证方法”对话框中勾选“匿名访问”复选框，然后单击右侧的“编辑”按钮。

有时网站管理员可能并不满意使用 IUSR_computername 作为匿名访问账号，出于安全考虑或管理方便，往往也需要指定另一个账号作为匿名访问账号。这时只需要单击“用户名”右侧的“浏览”按钮，并从“选择用户”对话框中指定新的匿名访问账号，单击“确定”按钮即可。

(9) 为 IIS 生成一个密钥对时，在任何域中不要使用逗号，原因是逗号被解释为字段的结尾。它们会在没有警告的情况下产生无效请求。

如果拥有多台具有 IIS 的虚拟服务器功能的 Web 服务器在安装证书时，要确定具体服务器的 IP 地址；否则系统创建的所有虚拟服务都适用同一个证书。

如果启动 SSL，任何指向支持 SSL 的 WWW 文件夹中文档的 URL 必须使用 https://，而不是在 URL 中的 http://。使用在 URL 中的 http://的任何链路不支持安全文件夹。

(10) 使用 IIS 随意向 INTERNET 发布信息时，要确保网络安全性。

**注意：**

① 为系统分区和各项 IIS 服务程序生成分开的区，这样黑客无法轻易地从某项服务程序的某个漏洞对整个机器访问。

② 对机器的所有分区使用 NTFS，要保证用户权限设置正确。

③ 将 IIS 服务器放置于其自己的域中，并与账户建立一种单向委托关系。如果黑客能得到某个有效账户的信息，那个账户也无法对用户域进行访问。

④ 为各项 INTERNET 服务使用单独账户(如果计划运行的不止是 Web 服务器的话)，这使得跟踪用户的活动相当容易。

⑤ 核查，然后再三核查为指定进行匿名访问的账户分配的权限和许可权。需要给用户分配最小的许可权，通常只是读许可权。

⑥ 只在 IIS 机器上存储非机密信息，并将信息放置在防火墙内。这样，如果信息安全性遭到破坏，黑客仍必须穿越防火墙。

⑦ 在服务器上使用 WINDOWS NT SERVER 的 TCP/IP 过滤功能，只允许连接到需要支持 IIS 服务的端口。比如，如果只想运行 Web 服务器只须启动端口 80。

⑧ 如果用户利用非匿名账户对服务器进行访问，务必通过加密密码进行验证。

### 5.3.4 Web服务的安全保障措施

#### 1. 用户名/密码的直接信任

该安全措施实现的基础是基于客户和服务器之间所建立的 SSL/TLS(secure socket layer/transport layer security)安全连接，由它来保证消息的机密性。同时通过 SSL 在被传输的消息中附加消息鉴别码 MAC (message authenticationcode)来提供消息身份验证，以鉴别消息在途中是否被修改以及消息创建者的身份是否被冒用。通信双方通过交

互握手过程，建立 SSL/TLS 安全连接，然后服务器把 User/Password 发送给客户。由客户构造 SOAP 消息，其中包括〈UsernameToken〉元素，该元素包含了客户使用服务的用户名和密码。服务器收到 SOAP 消息后，抽取〈UsernameToken〉元素并验证用户名和密码，如果验证成功，服务器处理消息并返回结果。

**2. 安全令牌和数字签名的直接信任**

该安全措施的实现基础是建立在公钥密码技术之上的安全令牌和数字签名。该措施假设通信双方已经使用某种信任机制（如 CA）建立了 Web 服务器对安全令牌的信任。实际运行中，服务器会核实并评估安全令牌。

消息发送方可能希望让接收方判别消息是否在传输过程中被更改，同时验证发送方的身份。发送方应该注意签署消息的所有重要元素，但在传送过程中可能被更改的部分不应被签署。标记对〈SignedInfo〉用来描述已签署的消息内容。由于对整个消息采用公钥算法加密会大大影响 Web 服务的性能，因此，实际中常使用一个摘要来加快处理速度。当消息被接收时，Web 服务的验证程序会验证重新计算的摘要与对方发送的摘要是否匹配。

**3. 基于文档的安全性**

该安全措施在非 SSL/TLS 环境下允许通过发送方和接收方共享的通用对称密钥，或消息中带有的加密形式的密钥，利用 XML 加密标记，对消息主体块、报头块、任意子结构和附件的组合进行加密。加密子元素中存在着解密需要的所有信息，如加密算法的名称、加密的数据类型和加密密钥的名称等，接收方可以根据这些信息识别加密部分并解密。

**4. 防火墙对 SOAP 消息的处理**

由于 SOAP 消息是封装在 HTTP 数据报中，这就给 Web 服务带来了潜在的安全隐患。可以利用防火墙适当过滤 SOAP 请求消息。

1）通过对 HTTP 请求标题字段的扩展标示出特定的 SOAP 消息

例如，在下面给出的 SOAP 请求代码中，定一个新的名为 SOAPAction 的 HTTP 请求标题字段，使得防火墙能够从普通的 HTTP 请求中识别出 SOAP 消息，然后进行相应处理。

```
POST/rpcrouter HTTP/1.1
Host: 127.0.0.1
Content-Type:text/xml;character="ufg-8"
Content-Length: 321
SOAPAction: "HTTP:// www. wrox. com/TimeService/GetDateTime"
<SOAP-ENV:Envelop>…</SOAP-ENV:Envelop>
```

2）防火墙利用 SOAP 安全性扩展标记实施更强的安全控制

该方式中，发送方另添加了一条〈Security〉报头块，把防火墙列为 SOAP 参与者，并

在路由报头块中指定路由信息。防火墙通过分析 actor 属性中特定指向防火墙的〈Security〉报头块，抽取安全令牌和数字签名，并做出响应。如果签名有效，并且授权消息是可信任的，则该消息即被许可；否则该消息就会遭到拒绝。

## 5.3.5 制定 Web 站点安全策略的原则

### 1. 设置安全 Web 站点的基本原则

为了确保 Internet 中 Web 站点的安全，应该为每个 Web 站点设置一个符合实际的安全策略，这些安全策略可能会因为 Web 站点的需求不同而有所不同。但制定安全策略的基本原则应该是相同的，即在满足网站基本安全需要的基础上，根据网站提供的服务和服务的对象来设置安全系统，评估和分析安全风险。在制定实际安全策略之前，应当首先分析网站可能遇到的安全威胁，再根据安全威胁列表制定切实可行的安全策略。下面是一个安全威胁列表的例子。实际应用是根据现场情况添加或修改。

(1) Web 站点有多少端口对外部开放？

(2) 对 Web 站点的可能威胁来自网络内部吗？

(3) 对 Web 站点的可能威胁来自网络外部吗？

(4) 如果黑客入侵 Web 站点，他可能访问站点中哪些数据库、哪些目录或文件？

(5) 系统中的数据被破坏是因为病毒，还是因为受到了黑客的攻击？

(6) 系统受到的攻击是哪种类型，例如，来自网络内外的非授权的访问、IP 地址欺骗或协议欺骗等？

网络安全威胁分析的结果可以作为系统管理员设计网络安全策略的基本依据，如果运用得当，可以增强网络的安全性。

### 2. 利用 Web 服务器记录客户信息

在 Internet 中 Web 服务器能够记录它们所收到的每一次连接和访问信息，这个记录通常包括发出连接请求的计算机的 IP 地址和主机名。如果用户在 Web 网站访问期间填写了任何表单，该表单下所有变量的值都会被 Web 服务器记录下来，例如，发出请求时的状态、所传送数据的大小和用户的 E-mail 地址等都会被 Web 服务器记录。这些记录对于分析客户机的性能，发现和跟踪黑客袭击是有用的。

## 5.3.6 配置安全的 Web 服务器

Web 服务器会给用户带来风险和损害，Web 客户机也会给 Web 服务器带来风险和损害。对于客户可能给服务器带来的风险，应注意服务器的安全。应确保客户只能访问他们有权访问的站点，如果发生了闯入，应有一些阻止闯入的措施。为了加强 Web 服务器的安全，应该采取下面的方法。

(1) 认真配置 Web 服务器，尽可能使用它的安全访问特性。

(2) 如果在 Windows 2000 Server 系统上运行 Web 服务器，应该检查驱动器和共享的权限，将所有系统资源设置为只读状态。

(3) 可将 Web 服务器中所有重要文件放在基本系统中,再设一个二级系统专门用于存放 Web 网站对外服务的数据和文件,存有重要数据的基本系统中的数据不向 Internet 开放。

(4) 按最坏的安全形势配置 Web 服务器系统。

(5) 最重要的是检查 Web 服务器使用的 Applet 脚本和 CGI 脚本,严格限制脚本的执行权限和执行范围,防止外部用户利用脚本执行 Web 服务器系统的内部指令。

### 5.3.7 及时消除 Web 服务器站点中的安全漏洞

无论是基于 Windows 2000 Server 系统的 Web 服务器,还是基于 UNIX/Linux 系统的 Web 服务器,都存在不同程序的安全漏洞。因此,系统管理员应该及时消除 Web 服务器站点中的安全漏洞,使安全漏洞对系统的影响降到最低。Web 服务器的安全漏洞通常有下面四种形式。

(1) 物理漏洞。主要由未经授权的人员在控制台上擅自使用 Web 服务器引起,由于能够从操作系统级访问系统,能够看到 Web 服务器站点的所有信息,并对 Web 服务器进行重新配置,这是十分危险的。例如,一台放置在比较开放的公共场所的 Web 服务器,就可能会遇到这种安全问题。

(2) 软件漏洞。主要是由系统管理员配置了"错误的 Applet 脚本和 CGI 脚本授权"引起的,一旦外来的脚本程序获得了系统程序执行的能力,它就可以控制系统、改变网络服务、对系统进行修改和破坏。系统管理员一定不要轻易相信脚本和 Applet 程序,尽可能不开放此项功能,如果一定要开放,请确保能够掌握它们的功能。

(3) 系统不兼容漏洞。主要是由系统软硬件集成不当引起的。原本安全运转的系统因为增加了一个新的硬件或新的软件时就可能会出现安全问题。这类问题很难被发现,往往是在系统受到攻击之后,系统管理员才会意识到是新装的软硬件惹的祸。因此,在重要系统安全新的硬件和软件之前,都必须先进行必要的测试。

(4) 没有制定必要的安全策略。如前所述,制定一个切实可行的安全策略是系统安全的根本保证。例如,某个 Web 服务器系统采用了十分可靠的密码安全认证体制,由于没有安全策略限制用户使用弱密码进行认证,用户为了方便记忆简单地使用了自己的名字或出生日期作为密码,那么系统的密码安全认证体制再完善也没有用。

### 5.3.8 严密监控进出 Web 服务器站点的数据流

Internet 上的 Web 服务器站点是任何人都可以通过浏览器访问的,它也是安全状况最难保证的系统。为了追踪闯入系统的黑客,需要严密监控进出 Web 服务器站点的数据流,可以在 Web 服务器上安装 Web 服务器统计软件监控进出 Web 服务器站点的数据流。此类工具软件能够列出网站被访问次数、站点上来往最频繁的用户以及站点的运行状态。一个 Web 服务器站点应该被严密监控的项目有下面几种。

**1. 监控 Web 服务器站点访问请求**

Web 站点是一种开放系统,在 Internet 上任何人都可以自由访问,访问者要访问某

个 Web 站点并无特别的理由,他可能是被丰富多彩的画面吸引,也可能仅仅是路过进来看看。在 Internet 上每个访问 Web 站点的人都希望自己能够尽快进入 Web 站点。一旦 Web 站点被挂在 Internet 上,就会有用户来访问和使用站点提供的各种服务。因此,通过监控可以获得很多有用的信息,有助于对 Web 服务器站点的安全管理。监控 Web 服务器站点访问请求主要包括以下几个方面。

(1) Web 服务器站点在正常情况下,每日被访问的次数是多少?

(2) Web 服务器站点被访问的次数突然大幅度增加了吗?

(3) Web 服务器站点在正常情况下,每日访问用户都是从哪里连接的?

(4) Web 服务器站点在正常情况下,每日何时最忙? 每周哪天最忙?

(5) Web 服务器站点上哪些栏目的信息被经常访问? 哪些网页最受欢迎? 每个目录下有多少网页被访问?

(6) Web 服务器站点上每个目录下每次有多少用户访问? 访问 Web 服务器站点的是哪些类型的浏览器? 与 Web 服务器站点进行交互的操作系统是哪种类型?

(7) 用户更愿意选择哪种提交方式与 Web 服务器站点进行交互?

以上信息对保证 Web 服务器站点的安全设置非常有用,网络管理员可以根据自己的需要适当地取舍。在选择监控软件时,应确保其与市场上流行的 Web 服务器兼容。

#### 2. 统计 Web 服务器站点访问次数

如果 Web 服务器站点管理员想了解 Internet 上有多少人知道 Web 站点,来访者到底关心哪些信息,实时统计 Web 服务器站点访问次数就十分重要。这个指标不但可以用于度量 Web 站点的成功度和知名度,而且也是 Web 服务器站点安全设置的重要参考值。

1) 确定 Web 服务器站点的访问次数

Web 服务器站点记录的访问次数是一个原始数字,它仅仅描述了 Web 服务器站点上文件下载的平均数目。例如,当一个用户在 Web 服务器站点上开始详细阅读信息时,一次简单的会话连接就会形成好几次访问记录,因此,访问次数将远远高于站点访问者的数目。

2) 确定 Web 服务器站点的访问者数目

Web 服务器站点管理员可以根据得到的站点的访问次数估算站点的访问者数目。如果将访问次数与主页文件联系在一起时,这个数字就接近于某个时期内访问者的数目,但也不是百分之百的准确。管理员必须明白站点的"访问次数"的本质,一个月有几十万次的访问记录并不意味着网站的成功。如果每个月访问次数都稳步增加,则说明这个 Web 服务器站点的成功度和知名度有所提高。

## 5.4 电子商务系统安全策略

随着互联网的发展,计算机网络在经济和生活的各个领域迅速普及,整个社会对网络的依赖程度越来越大,众多企业以及其他组织或机构都在组建和发展自己的网络并连

接到 Internet 上，以充分共享和利用各种信息和资源。伴随着网络的发展，也产生了各种各样的问题，其中安全问题尤为突出，网络安全的重要性也越来越受到关注。一般来讲，计算机网络安全防御技术可以分为以下几种：(1)物理安全技术。(2)运行安全技术。保障运行安全的主要技术和机制有防火墙及身份认证技术、网络安全检测与监控等。(3)信息保护技术。保障信息安全涉及加密技术、访问控制与认证技术、数字签名、数据完整性技术等。其中，加密技术是核心。

对于企业网络，一般采用防火墙作为安全的第一道防线，而随着攻击者知识的日趋成熟以及攻击工具与手法的日趋复杂多样，单纯的防火墙策略已经无法满足网络安全的需要。同时，企业内部网络同样也存在很大的安全威胁。统计结果显示企业网络遭受更多的是来自内部的攻击，外部攻击只占约 39%。

企业信息化应用的信息安全隐患主要包括：

(1) 身份认证。企业网站无法验证登录到网站上的客户是否是经过认证的合法用户，登录到企业网站的客户或企业员工也无法知道所登录的网站是否可信，非法用户可以借机进行破坏。“用户名＋密码”的传统认证方式安全性较弱。

(2) 信息的机密性。在企业内部和外部网络上传输的企业敏感信息和数据有可能在传输过程中被非法用户截取。

(3) 信息的完整性。敏感机密的信息和数据在传输过程中有可能被恶意篡改。

(4) 信息的不可抵赖性。企业的财务报表、客户购货信息、购销合同、生产数据等电子文件和数据信息一旦被一方所否认，另一方则没有已签名的记录来作为仲裁的依据。

### 5.4.1 电子商务概述

目前，电子商务已成为世界范围内新的研究热点。但是电子商务的安全性是实施中的关键问题，也是技术难点。本章主要介绍电子商务的概念、电子商务的安全性要求，并通过电子支付系统、电子现金系统详尽介绍电子商务的安全技术，最后介绍电子现金协议的实现方法及电子商务业务系统应用系统实例。

#### 1. 电子商务的概念

Internet 在商务领域引起一场巨大的革命，电子商务已成为人们关注的焦点之一。电子商务的早期形式是 EDI(电子数据交换)。EDI 的主旨是商务票据传送的电子化，由于使用者少、应用范围小，没有人称其为电子商务。从 20 世纪 80 年代初开始，世界范围内使用 Internet 的人数迅速增长，为电子商务的发展和广泛应用提供了良好的基础，电子商务一词才被提出，而且受到学术界、商业界和产业界的热切关注，各国政府也给予电子商务发展以极大的关注和支持。

从广义上讲，电子商务是指通过电子数据交换来完成某种与商务或服务有关的工作，它可以是各种形式、各种内容、各种目的、各种风格、各种程度的电子数据的交换，其基础是以电子化的形式来处理和传输商务数据，包括文本、声音、视频、图像等数据类型。电子商务有许多不同的内容，例如，货物贸易和相关服务、提供数字化的商务材料、实现电子转账、完成电子化的股票交易处理、提供电子提货单证、进行商业买卖活动、不同的

工程设计人员协同完成工程设计、联机科技情报查询服务等。

直观地说，电子商务就是将传统商务移植到信息网上。与传统商务相似，电子商务为销售者和消费者建立交易关系，使他们能商谈交易的商品和交易的条件，如提供何种商品或服务、适应的法律和规范、价格、付款方式、商品提供方式和保证等。

实际上，电子商务主要包含三个要素：信息、电子数据交换和电子资金转账。其系统构成如图5-9所示。




**图5-9 电子商务系统组成**

电子商务的交易过程可以描述为三个阶段。

(1) 交易前。主要是指交易各方在交易活动前的准备活动，包括网络咨询、广告、商务洽谈等。

(2) 交易中。包括合同的签订，涉及企业间、公证机关、银行、税务、海关等方面的电子凭证交换，即电子数据交换和电子支付。

(3) 交易后。包括商品的支付、电子支票等。

与传统的商业系统相比，电子商务具有交易花费成本低、资金更安全、资金结算速度快、节省人力物力、方便等特点。由于在电子商务操作过程中涉及金钱交易等信息，因此不允许在传送过程中有第三者的窃听、篡改、伪造，也不允许对其进行非法访问。要使电子商务发挥其巨大的潜力，应对所有网络用户都是开放的，且至少应像传统商务那样方便、可靠和安全。

### 2. 网络环境

网络环境是开展电子商务的基础。信息的传递、网上资金账户的认证、资金的划转等都需要数据交换的网络环境。

现在的电子商务发展是以Internet技术为基础的，这样可以节约很多成本。所以，企业所在地区Internet的发展情况会直接影响企业开展电子商务的业务。利用Internet开展电子商务，对网络的要求很高，不止是Internet环境存在就可以，其稳定性、带宽以及接入费用都对电子商务的开展有举足轻重的作用。

### 3. 支付系统

利用现在的网络获取商务信息，但在进行商品交易时还不得不借助于传统的银行业务系统，即支付手段不能在网上进行时，无疑会使交易的支付成为电子商务进一步发展的“瓶颈”。网上银行以及网上支付系统的建立与完善也是电子商务发展的重点条件之一。

虽然网上银行与支付系统的发展不是目前各个商业企业所能决定的事情，但随着电子商务的进一步发展和金融环境的逐渐优化与完善，企业在时机成熟时和网上银行建立合作关系可以解决商务中的资金流的问题。

### 4. 安全认证系统

传统的商务活动是以现有的信用体系为依托，比如票据、现金、对方企业的实力及担保等。但是，电子商务的主要形式之一就是网上交易，包括合同的处理以及资金的划转等，所以在网上怎么确定信用、如何保护商业秘密、如何保证网上账户的数据传送的安全，对发展电子商务是一个很严重的问题。

## 5.4.2 电子商务安全的主要问题

电子商务实质是电子方式的贸易活动，它利用简单、快捷、低成本的电子通信方式，使买卖双方进行各种商贸活动的新型贸易形式。它不仅改变了企业本身的生产、经营、管理活动，而且将导致人类经济、社会和文化的一次新的革命。

电子商务安全的主要问题有以下几个方面。

### 1. 篡改

电子的交易信息在网络上传输的过程中，可能被他人非法地修改、删除或重放(指只能使用一次的信息被多次使用)，从而使信息失去了真实性和完整性。

### 2. 信息破坏

包括因网络硬件和软件的问题而导致信息传递的丢失与谬误，以及一些恶意程序的破坏而导致电子商务信息遭到破坏。

### 3. 身份识别

如果不进行身份识别，第三方就有可能假冒交易一方的身份，来破坏交易、败坏被假冒一方的声誉或盗窃被假冒一方的交易成果等。而且不进行身份识别，交易的一方可以不为自己的行为负责任，进行否认，相互欺诈。

### 4. 信息泄密

主要包括两个方面，即交易双方进行交易的内容被第三方窃取或交易一方提供给另一方使用的文件被第三方非法使用。

### 5.4.3 电子商务的安全技术

由于电子商务涉及金融、企业商家等各个方面的利益，所以，必须采用行之有效的手段来保证电子商务系统的安全运行。安全性技术是保证电子商务健康有序发展的关键因素，也是目前大家十分关注的问题。虽然 Internet 的开放式的信息交换使之在安全方面存在脆弱性，但现在几乎网络的各个层次都制定了安全协议和具备了相应的安全技术，以保证电子商务的安全性。电子商务的安全性策略可分为两大部分，一部分是计算机网络安全；另一部分是商务交易安全。电子商务中的安全性技术主要有以下几种。

**1. 信息保密技术**

信息保密就是使敏感信息不被非授权的人知道。电子商务中的信息保密，主要是指发送方必须使信息在通过网络向接收方传递的过程中，保持一种只有该合法接收方才能理解的形式。就是说，发送方必须在发送前对信息进行加密。加密就是对信息进行编码使其看起来毫无意义，同时仍保持其可恢复的形式。这种对信息行编码的方法称为加密算法。加密算法将需要保护的原始信息称为平文或明文，用一种称为密钥的数值进行编码，生成的结果称为密文。尽管他人完全可能知道所使用的加密算法，但要对密文进行解密就必须有创建明文的正确密钥。

由于加密算法有太多可能的密钥，使得在设计一个加密算法时，要对这些可能的密钥一个个地尝试找出哪一个是正确的密钥变得完全不可行，因而加密的信息得到了保护。一般的加密模型如图 5-10 所示。

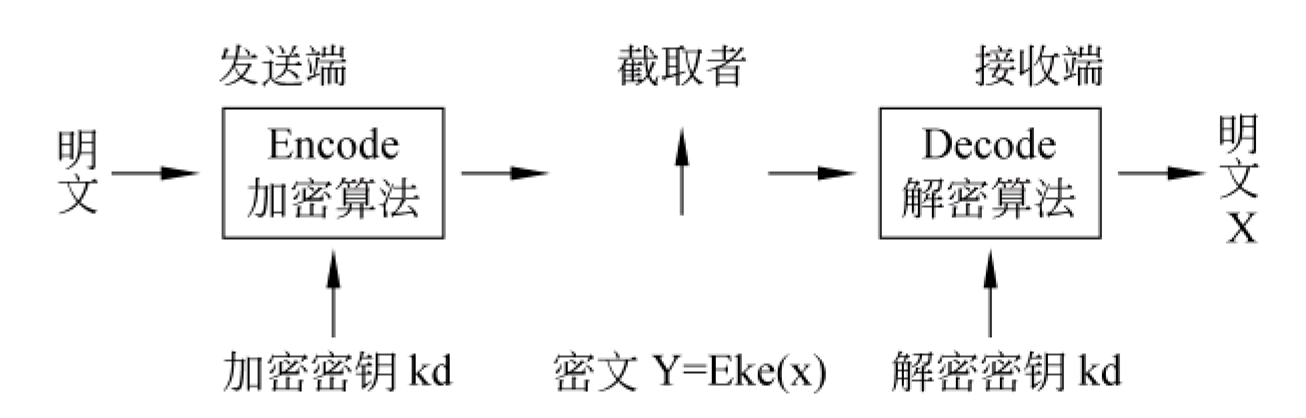



**图 5-10 加密模型示意图**

在发送端，发送者用加密密钥进行加密。而在接收端，接收者则用相应的解密密钥进行解密得到明文。迄今为止，人们已提出了许多加密算法，但通常使用的只有 DES、PC4、IDBA、RSA 等少数几种，并将这些算法归纳为两类基本算法，即对称密钥加密算法和非对称密钥加密算法。

对称密钥加密算法，是因为在使用这种算法的系统中对信息加密和解密使用同一密钥。由于加、解密使用相同的密钥，所以，该密钥必须处于保密状况，因此，其可称为秘密密钥。该算法又可称为秘密密钥加密算法。由于为保密起见秘密密钥经常进行改变，又由于它主要用于文件会话中，所以又称它为会话密钥。

而非对称密钥系统与对称加密算法不同，它需要使用一对密钥——公开密钥和私有密钥。如对数据加密用的是公开密钥，则需用对应的私有密钥进行解密。如用私有密钥对数据进行加密，则只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不

同的密钥，所以，这种算法称为非对称密钥加密算法。公开密钥和私有密钥成对产生、成对使用，同时非对称加密算法保证了从公开密钥不可能推导出私有密钥。

对称密钥加密算法计算速度快，性能较好，被广泛应用于对大量数据的加密，如对文件的加密。而非对称密钥加密算法计算机速度较慢，但在系统保密性能上要优于对称加密算法。一般在实际使用中是将两种算法结合使用，从而产生了数字信封技术。发送方使用对称加密算法和秘密密钥加密数据文件，生成文件密文，使用非对称加密算法和接收方的公开密钥加密发送方的秘密密钥，生成数字信封。发送方将文件密文和数字信封同时发送给接收方。接收方则首先使用自己的私有密钥解密数字信封，得到发送方的秘密密钥，再使用秘密密钥解密文件密文，得到文件明文。

常用的属于对称加密算法的有 DES、RCR、IDEA 等，其中 DES 使用得最为普遍，已被 ISO 采用作为数据加密标准。DES 是使用 56 位长的密钥进行加解密的。在非对称加密算法中常用的有 RSA，已被 ISO/TC 的数据加密技术分委员会 SC20 推荐为非对称密钥数据加密标准，所使用的密钥长度一般为 769～1024 位。DES 和 RSA 数据加密技术已被广泛应用于电子商务交易系统中，使得敏感信息在网上传送的保密性得到了很大的提高。

**2. 完整性控制技术**

数据加密技术能使敏感信息在网上传输过程中处于保密状态，不被非法窃取。但如果信息密文在传输过程中被非法篡改，那么用户在正确解密后得到的却是错误的明文信息。完整性控制技术就是要使得接收方所收到的信息与发送方所发送的信息保持一致。完整性控制的核心是完整性验证，这就要求首先必须采取某种措施，使得用户能够验证网上传送来的信息是否完整，即验证所收到的信息是否与发送方所发送的信息保持一致，若发现信息完整性被破坏就可要求发送方重新发送。通常所采取的完整性验证技术有两种，冗余密文和设置检测向量。

冗余密文就是使用某种加密算法对报文进行加密计算而得到的与报文唯一对应的数值。该加密算法必须具有很好的单向性和置乱性。单向性就是由冗余密文来构造原报文是不可行的；置乱性就是该加密算法必须对原报文的极小变化非常敏感，一旦有微小变化，相应的冗余密文也会“面目全非”。发送方将报文密文和冗余密文封装在一起发送。在传输过程中由于黑客不能对报文解密，所以，也就无法既修改报文数据又产生新的冗余密文。这样，用户在收到密文信息后，首先解密报文密文，再重新产生冗余密文，并将其与发送来的冗余密文进行比较。若不相等，则说明接收方所收到的报文与发送方所发出的报文内容不一致，报文的完整性受到破坏；若相等，则说明报文在网络传输过程中保持了完整性。

设置检测向量，是指对报文信息名字段（或域）按一定的算法进行计算操作，得到一个约束值，称为该报文信息的完整性检测向量（integrated check vector，ICV），然后将它与报文信息封装在一起进行加密。在传输过程中，由于黑客不能对报文解密，所以也就不能既修改报文数据又计算新的 ICV。这样，接收方收到报文后解密并计算 ICV 将其与报文中的 ICV 字段进行比较。若不等，说明报文信息的完整性受到破坏。只有在相等的

情况下，才确认报文有效。

上述两种完整性验证技术的着眼点都是提供某种检测标准，根据这些检测标准可以发现报文被修改过的蛛丝马迹。当发现信息不完整时，即可要求对方重新发送来确保网上传送信息的完整性。在电子商务实践活动中，冗余密文完整性控制技术应用得比较广泛。通常人们是使用安全 Hash 编码法(secure hash algorithm，SHA)对明文进行计算操作得到一定长的 128bit 的冗余密文。这就是通常所称的数字摘要技术，所得到的 128bit 的密文称为消息摘要或数字指纹。

### 3. 数字签名技术

在电子商务活动中，人们是通过网上信息的传送来完成交易过程的。它一方面提高了商业活动的效率；另一方面也给欺诈行为的发生留下了很大的空间。

在传统的以书面文件为基础的处理中，为防止这些欺诈行为采取了交易双方在书面文件上签名的方法。书面签名的形式包括手写签名、印章、指印等。但无论是何种形式的签名都必须符合非伪造性和可鉴别性这两个基本要求。这样在对文件签名之后如果出现纠纷，有关当事人只需向某公证机构出示签名文件。由它来鉴别签名，判定文件是否真实有效，并据此明确双方的权利、义务和责任，从而有效地解决纠纷，制止欺诈行为。

在电子商务活动中交易双方使用电子文件来记载各交易事项，面对电子文件就必须采取数字化的签名方式，即数字签名。虽然数字签名采取了二进制数字技术，但作为签名方式之一，它还是必须达到所有签名方式都应达到的要求。

(1) 接收方或非法者不能伪造签名和篡改文件。

(2) 接收方能够鉴别发送方的真实身份。

(3) 发送方事后不能对自己发送文件行为进行抵赖。

现代数字签名技术以加密技术为基础，采用加密技术的加解密算法体制来实现对报文的数字签名。具体实现数字签名的方法很多，但在目前电子商务实践中使用最广泛的是非对称密钥数字签名技术。

使用这一技术进行数字签名时，签名人首先利用单向 Hash 函数产生所要签署的电子文件的消息摘要，再使用自己的私有密钥加密该消息摘要，所得结果即为签名人对该电子文件的数字签名。签名人可将文件和数字签名一起发送给接收方，接收方可用签名人的公开密钥解密数字签名，得到文件的消息摘要，从而可验证文件是否完整。

一般为了实现在公开网络上的安全传输，人们同时使用了数字签名技术和信息加密技术。下面简单分析数字签名和信息加密的文件传输过程。

(1) 发送方首先使用单向 Hash 函数从原文得到消息摘要，然后使用发送方的私有密钥对消息摘要进行加密，得到数字签名，并将数字签名附加在要发送的原文之后。

(2) 发送方选择一个秘密密钥对文件进行加密，并将加密后的文件通过网络传送到接收方。

(3) 发送方用接收方的公开密钥，对秘密密钥进行加密，生产数字信封，并通过网络将数字信封传送到接收方。

(4) 接收方使用自己的私有密钥解密数字信封，得到秘密密钥。

(5) 接收方使用秘密密钥解密文件密文,得到文件明文和数字签名。

(6) 接收方使用发送方的公开密钥解密数字签名,得到文件的消息摘要。

(7) 接收方使用单向 Hash 函数对文件明文重新计算产生消息摘要。并将它与解密后的消息摘要进行比较。如果两个摘要相同,则说明文件在传输过程中没有被破坏。

从上述过程可以看出,非对称密钥签名技术完全可以满足电子商务对数字签名所提出的要求,是一种行之有效的数字签名技术。

从开放网络上的安全传输过程可见,数字签名的加解密过程和秘密密钥的加解密过程虽然都使用公开密钥体系,但实现的过程正好相反,使用的密钥对也不同。数字签名使用的是发送方的密钥对,即发送方用自己的私有密钥进行加密,接收方用发送方的公开密钥进行解密。这是一个一对多的关系,任何拥有发送方公开密钥的人都可以验证数字签名的正确性。而秘密密钥的加解密则使用的是接收方的密钥对,这是一个多对一的关系,任何知道接收方公开密钥的人都可以向接收方发送加密信息,只有唯一拥有接收方私有密钥的人才能对信息解密。在实用过程中,通常一个用户拥有两个密钥对,一个密钥对用来进行数字签名;另一个用来对秘密密钥进行加密解密。这样,数字签名和信息加密分别使用不同的密钥对,为系统提供了更高的安全性。

**4. 身份认证技术**

身份认证是证实一个声称的身份或角色(如用户机器、节点等)是否真实的过程,它是实现授权、审计等访问控制过程的必要条件,是计算机网络安全系统不可缺少的组成部分。

认证技术主要依赖于对象知道的东西(如密码、PIN 值)、对象拥有的东西(如 IC 卡、信物)和对象的生物统计学上的特征(如指纹、声音)。

现在一般采用的是第一种认证技术,即使用只有合法用户才知道的密码来认证用户身份。显然在网络上传送密码是不安全的,必须引入加密技术对认证过程进行保护,这就要涉及不同的密钥系统。

对称密钥系统是最早被应用于认证过程的密钥系统。使用对称密钥加密技术的认证系统往往需要引入一个可信第三方,由其充当认证权威,为系统中每个合法用户分配一个唯一性的标识名和秘密密钥,并负责对它们进行管理,而且它还要在通信双方相互认证的具体过程中发挥关键性的作用。下面简单地分析一下这类系统的原理。

认证服务器(authentication server,AS)为可信第三方;A、B 为两个需要通信的系统用户;INA、INB 分别为 A、B 两个用户的标识名;KA、KB 分别为 A、B 两个用户的秘密密钥;T 表示系统时间;{……}K 表示用密钥 K 加密{}中的数据。

(1) 用户 A 向认证服务器 AS 发送通信请求,请求信息中包括了 INA、INB。

(2) 认证服务器 AS 根据 INA、INB 找到分配给用户 A 和用户 B 的秘密密钥 KA 和 KB,然后为用户 A 和用户 B 的此次通信分配一个会话密钥 K,并生成{INB,K}KA 和{INA,INB,K}KB,将这些加密信息发送给用户 A。

(3) 用户 A 接收到 AS 发来的请求信息后,首先输入自己的密码,若输入的密码正确即可使用 KA 解密{INB,K}KA,得到会话密钥 K,然后生成{INA,T}K,并将其和{INA,

INB,K}KB一起发送给用户B。

(4) 用户B输入自己的正确密码后,使用KB解密{INA,INB,K}KB,得到K,再用K解密{INA,T}K,并验证所收到的信息是否一致。若一致即证明了通信对方是具有标识名INA的合法用户A。

(5) 用户B生成应答信息{INB,T}K,发送给用户A。

(6) 用户A使用K解密{INB,T}K,并验证用户B发来的信息与AS发来的信息是否一致。若一致即证明了通信对方是具有标识INB的合法用户B。此后,双方即可使用会话密钥K进行保密通信。

由上述可见,此类认证系统的特点是由可信第三方为每个合法用户分配一个秘密密钥,而该秘密密钥就作为特殊的密码起着验证每个进入系统的用户是否具有合法身份的作用。但这类认证系统的明显缺陷是,可信第三方容易形成系统性能"瓶颈",这就决定了这类认证系统只是在中小规模的网络系统中得到广泛的应用。

随着大规模网络系统的发展,特别是在Internet网络出现后,非对称密钥加密技术逐渐被应用于认证系统之中。其标志就是数字签名技术被用于身份认证过程。但数字签名只能够将签名人与他声称具有的身份和公开密钥对应起来,而完整的身份认证过程则还应包括对用户声称具有的身份和公开密钥的合法性进行确认。只有这样才能证明签名人不仅具有确认的身份,还具有合法的身份。这样的工作仅靠通信的双方是不能胜任的,而必须由一个大家都信任的第三方认证机构来承担。为此引入了认证中心(certification authority,CA )和证书(certification)这两个概念。

CA是一个受大家信任的第三方认证机构,用户向CA提交自己的公开密钥和其他代表自己身份的信息,CA验证了用户的有效身份之后,向用户颁发一个经过CA私有密钥签名的证书。证书就是一个文档,它记录了用户的公开密钥和其他身份信息。

这样,两个用户在通信前可以相互交换证书,了解对方所声称具有的身份和公开密钥。由于每份证书上都有CA的数字签名,用户可以用CA的公开密钥解密数字签名,得到证书的消息摘要,再对证书重新计算消息摘要,最后将两条摘要相比较,若相等则说明数字签名是有效的,证书确实是CA所签发的。从而对方所声称具有的身份和公开密钥者是真实的、合法的。这一步完成之后,双方再相互交换文件和数字签名,并根据数字签名验证对方的确是所声称具有的身份和公开密钥的真正拥有者,这样就可判定签名人具有确定的合法身份,从而完成了整个认证过程。

CA用来为用户签发证书,提供身份认证服务,是整个系统的安全核心。在非对称秘密密钥认证系统中,用户的签名密钥和加密密钥通常是分开的,而CA只知道用户的签名公钥,这样就降低了CA受到攻击的危害程度,避免了可信第三方被攻击整个系统即陷入瘫痪的严重问题。此外,在认证系统中CA只负责审核用户的真实身份并对此提供证明,而不介入具体的认证过程,从而缓解了可信第三方的系统"瓶颈"问题,而且CA只需管理每个用户的一个公开密钥,大大降低了密钥管理的复杂性。这些优点使得非对称密钥认证系统用于用户众多的大规模网络系统。

为了与大规模网络系统的用户众多且分布广泛的特点相适应,CA也采用了分布式和分级信任的体系,即将所有用户分成若干个用户群,每个用户群有一个专门的CA为其

提供身份认证服务和签发证书。这是第一级的CA，对它们又可划分成不同的组，每组第一级CA又有一个专门的第二级CA为其签发证书，提供认证服务；以此类推，直至到达一个最高级CA，由它为所有它的下一级CA签发证书，提供认证服务。CA内部呈现为倒树形结构，顶部的最高级CA也可称为根CA，而且在一个认证系统中只能有唯一的根CA，它是所有各方都绝对信任的认证权威。

在这样一种分级信任体系中，一个用户不仅可以检查对方用户的身份，还可检查为对方用户颁发证书的CA的身份，并可沿着分级信任的层次结构对各级CA的身份都进行验证，直到根CA为止。这种分级信息的非对称密钥认证系统已成为Internet网络上的主流认证系统。

### 5.4.4 电子支付系统的安全技术

#### 1. 电子支付系统的安全要求

利用电子商务进行商品交易，必然会牵涉到支付。随着Internet的日益普及，已开发出了很多网上支付系统。“网上支付”顾名思义是通过网络进行货币支付，其本质是试图在网上把现有的支付结构转化为电子形式。例如，国外的实物商品零售应用系统大都采用了支票处理方式，从而避免了大量的纸张处理。而信用卡行业已建立了一系列的设施，使得在大范围内实现信用卡联机服务。在电子现金方面，出现了许多新的现金形式，这些新的现金形式往往是为支持特定的购买者和销售商之间的关系而设计的。

货币的不同形式导致了不同的支付方式。一个安全、有效的支付系统是实现电子商务的重要前提，它应有以下功能。

(1) 使用X509和数字签名实现对各方的认证。

(2) 使用加密算法对业务进行加密。

(3) 使用消息摘要算法以保证业务的完整性。

(4) 在业务出现异议时，保证对业务的不可否认性。

(5) 处理多方贸易的多支付协议。

为了实现协议的安全性，必须对参与贸易的各方身份有效性进行认证。例如，客户必须向商家和银行证明自己的身份，商家必须向客户及银行证明自己的身份，示意图如图5-11所示。

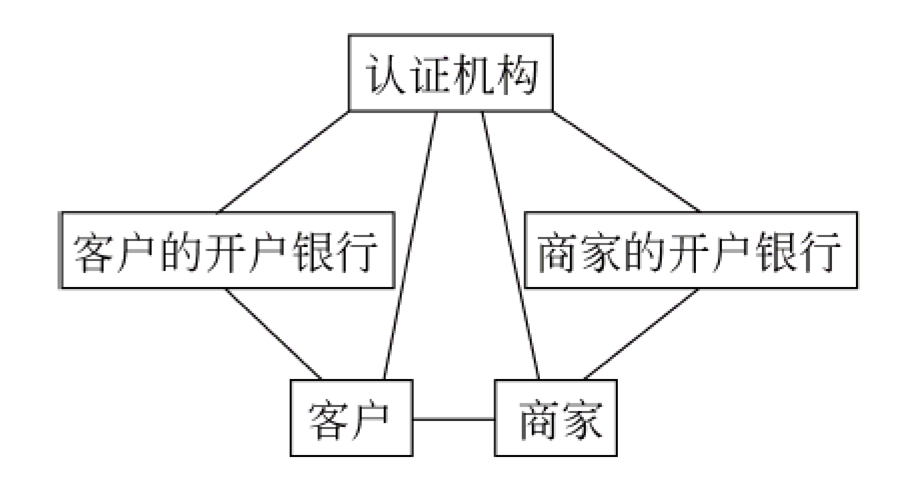



**图 5-11 认证方之间示意图**

其中，商家的开户银行表示商家在其中有账号的某财政机构，称为接收行。支付网关是由接收行操作的用于处理商家支付信息的设备。证书发放机构CA的职能是向各方发放X509证书。在某些接收行也可能有自己的注册机构，由注册机构向商家发放证书，商家可向客户出示这个证书以向客户说明自己是合法的。认证机构和注册机构的工作应是协调的。

为实现保密，系统应支持某些加密方案。在使用网页浏览器和服务器的同时，系统可利用安全套接字层SSL和安全的超文本传输协议S-HTTP。根据需要，加密算法可使用单钥或公钥算法，通过利用加密和消息摘要算法，以获得数据的加密和数据的完整性。

业务的不可否认性是通过使用公钥体制和X509证书体制来实现的。业务的一方发出他的X509证书,接收方可从中获得发送方的公钥。此外,每个消息可使用MD5单向杂凑算法加以保护。发送方可使用自己的秘密密钥加密消息的摘要,并把加密结果一同发送给接收方。接收方用发送方的公钥证实发送方的确已发出了一个特定的消息,然后发送方可计算一个新的秘密密钥用于下次加密消息摘要。

多支付协议应满足以下两个要求:这些要求可加强传统支付方案的安全性,商家只能读取订单信息,如货物的类型和销售价。接收行对支付认证,商家就不必读取客户信用卡的信息了。接收行只需知道支付信息,无须知道客户所购何物。在客户购买大额物品时可能例外。

### 2. 电子支付手段

典型的电子支付手段有电子信用卡、电子支票、电子现金。

1) 电子信用卡

在早期的Web站点商务应用中,只是要求输入信用卡号码,然后把这个号码以明码方式通过Internet传送给清算系统,以获得确认。显然,这种方式的安全性是有问题的。其后,为了提高联机信用卡的安全性,采取了一系列的技术。

首先,在Netscape和Microsoft的Web的设施中,都实现了安全套接字层SSL。SSL保证在浏览器与Web服务器间的通信信息不会被第三方获取。这样有效地防止了通过监听网络来收集信用卡号码或修改有关交易报文的可能。

图5-12是电子信用卡系统示意图。

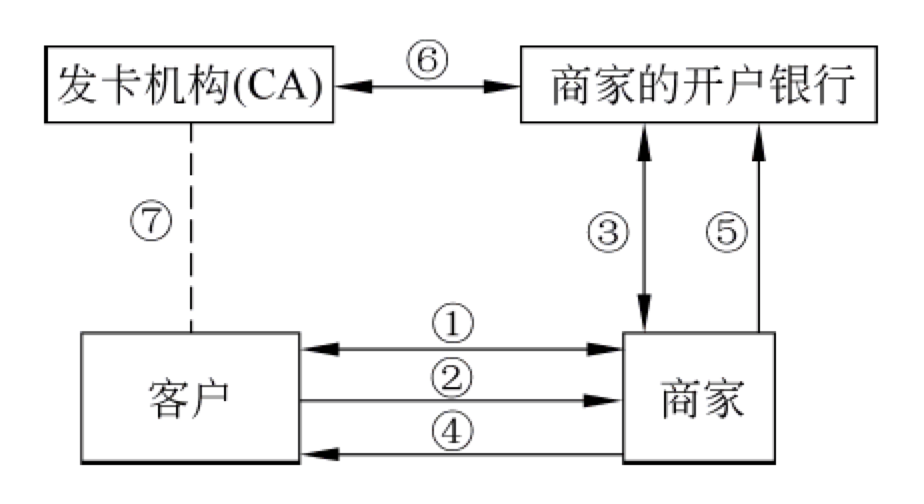


**图5-12 电子信用卡系统运行流程**

系统的参与者共有四方:具有Web浏览器的客户;处理信用卡业务并提供主页的商家服务器;为商家处理信用卡业务的商家的开户行;发卡机构。

使用信用卡的业务过程分三个阶段。

第一阶段完成客户的购物。客户访问商家的主页,得到商家货物明细单。客户挑选所需的货物,并用信用卡向商家支付。商家服务器访问其银行,对客户的信用卡号码及所购货物的数量进行认证。银行完成认证后,通知商家购物过程是否向下继续进行。商家通知客户业务是否已经完成。

第二阶段从客户账目向商家账目转账。商家服务器访问商家的开户行,并向银行提供购物的收据。商家银行访问发卡机构以取得商家所得到的现金。

第三阶段通知客户应支付的款额,并为客户下账。发卡机构根据一段时间内(可能一个月)客户购物时应向各商家支付的款额,为客户下账,并通知客户。

2) 电子支票

电子支票系统用于发出支付和处理支付的网上服务。付款人向收款人发出电子支票,收款人将其存银行以取出现金。每宗业务都是在Internet上进行的。电子支票与通常支票工作方式大致相同,它具有一种类似的电子签名,常规的加密方式使得电子支票

和通常的支票都适用于信用卡无法处理的小额支付。目前已开发的许多系统是为那些通过 Internet 出售信息或小型软件程序的公司而设计的。几乎所有的方案都依赖第三方或经纪人，他们证实客户拥有买货的款额，也可以证实在客户付款前，商家已交货。由于这个过程高度自动化，即使是交易额小到一分，这种方式也很经济划算。

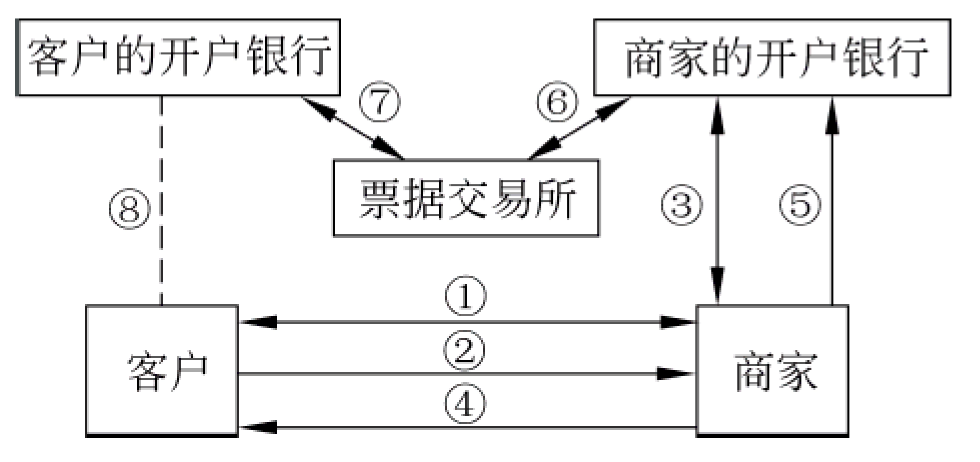


图 5-13　电子支票系统运行流程

图 5-13 是电子支票系统的描述。系统中主要的各方有客户、商家、客户的开户行、商家的开户行，票据交易所可由一独立的机构或现有的一个银行系统承担，其功能是在不同的银行之间处理票据。

客户使用一种访问 Internet 上不同 Web 服务器的浏览器，可浏览网上的商店。该浏览器同时还可向用户显示电子支票的格式。

一宗完整的电子支票业务由下面略述的若干步构成，这些步骤可分为三个不同阶段，如图 5-13 所示。

第一阶段购买货物。客户访问商家的服务器，商家的服务器向客户介绍其货物。客户挑选货物并向商家发出电子支票。商家通过其开户银行对支付进行认证，验证客户支票的有效性。如果支票是有效的，商家则接收客户的这宗业务。

第二阶段把支票存入商家的开户银行。商家把支票电子化发送给它的开户行。商家可根据自己的需要，何时发送由其自行决定。

第三阶段不同银行之间交换支票。商家的开户行把电子支票发送给交易所以兑换现金。交易所向客户的开户行兑换支票，并把现金发送给商家的开户银行。客户的开户行为客户下账。

与传统的纸支票和其他形式的支付相比，电子支票有以下优点。

(1) 节省时间。电子支票的发行不需要填写、邮寄或发送，而且电子支票的处理也很省时。在用纸支票时，商家必须收集所有的支票并存入其开户行。用电子支票，商家可即时发送给银行，由银行将其入账。所以，使用电子支票可节省从客户写支票到为商家入账这一段时间。

(2) 减少了处理纸支票时的费用。使用电子支票可免除诸如每月第一天在银行的排长队，大学新学期缴学费时的排长队。相应地，减少了银行职员在收支票、处理支票以及向客户邮寄注销支票时的工作。

(3) 减少了支票被退回情况的发生。电子支票的设计方式使得商家在接收前，先得到客户开户行的认证，类似于银行本票。

(4) 电子支票在用于支付时，不必担心丢失或被盗。如果被盗，接收者可要求支付者停止支付。

(5) 电子支票不需要安全的存储，只需对客户的秘密密钥进行安全存储。

(6) 电子支票也有某些保密性方面的考虑。电子支票必须经手银行系统，银行系统对经手的每宗业务必须用文件证明其细目。同时必须为被支付者保密，不可泄露业务的细节。

3）电子现金

电子现金又称为数字现金，是能被客户和商家接受的、通过 Internet 购买商品或服务时使用的一种交易媒介。

系统中有一电子现金的发行银行，记为 E-Mint。它根据客户所存款向客户兑换等值的电子现金，所兑换的电子现金须经数字签字。客户可用 E-Mint 发行的电子现金在网上购物。

图 5-14 是系统中的各方及其关系的描述，其业务可分为独立的三个阶段。

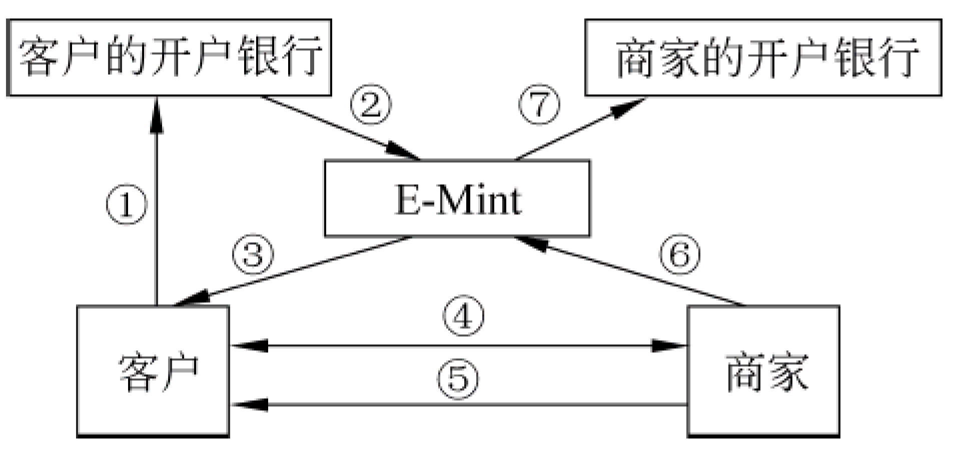


图 5-14 电子现金系统运行流程

第一阶段获得电子现金。客户为了获得电子现金，要求他的开户行把其存款转到 E-Mint。客户的开户行从客户的账目向 E-Mint 转账。E-Mint 给客户发送电子现金。客户将电子现金存入其计算机或 Smart 卡。

第二阶段用电子现金购物。客户挑选货物并且把电子现金发送给商家。商家向客户提供货物。

第三阶段商家兑换电子现金。商家收到电子现金发送给 E-Mint，或者商家把电子现金发送给他的开户银行，由开户银行负责在 E-Mint 兑换。E-Mint 把款项划到商家的开户银行，商家的开户银行为商家入账。

以上过程是在客户和商家之间进行的。类似地可用于在两个客户或两个机构如银行、学校、企业之间进行。

### 5.4.5 电子商务安全策略

随着互联网的不断发展，在世界范围内掀起了一股电子商务热潮。许多国家的政府部门对电子商务的发展十分重视。中国对电子商务的发展也给予了应有的重视，考虑到电子商务必然涉及网上支付及银行支付结算，为了做好前瞻性的研究，中国人民银行支付科技司早在 1998 年 6 月就组织成立了电子商务课题组对银行支付在电子商务中的作用和对策进行研究，并在研究基础上，组织各商务银行联合共建金融认证中心，即 CA 中心，为网上安全支付创造了条件。实现电子商务的关键是要保证商务活动过程中系统的安全性，即应保证在向基于 Internet 的电子交易转变的过程中与传统交易的方式一样安全可行。电子商务的安全主要采用数据加密和身份认证技术。下面主要从认证系统、SSL 协议和安全电子交易 SET 协议 3 个方面来加以论述。

#### 1. 认证系统

电子商务的关键是安全，网上安全交易的基础是数字证书。证书类似于现实生活中的身份证，用以在网络上鉴别个人或组织的真实身份。证书的颁发机构叫做 Certificate Authority，通常简称为 CA。要建立安全的电子商务系统，必须首先建立一个稳固、健全的 CA；否则一切网上的交易都没有安全保障。传统的对称密钥算法具有加密强度高、运算速度快的优点，但密钥的分发与管理问题限制了它的应用。为解决此问题，20 世纪

70 年代密码界出现了公开密钥算法(rivest shamir adleman，RSA)。RSA 算法是公开密钥算法中研究最为深入,使用最为广泛的算法,为大多数国家(地区)的官方或非官方所采用。整个认证系统是一个大的网络环境,系统从功能上基本可以划分为 CA、RA(证书的登记机构)和 WP(证书的分页系统)。

1) 认证系统的基本原理

20 世纪 70 年代密码界出现的公开密钥算法使用一对密钥,即一个私钥和一个公钥。其对应关系是唯一的,公钥对外公开,私钥个人秘密保存。一般用公钥来进行加密,用私钥进行签名。同时私钥用来解密,公钥用来验证签名。算法的加密强度主要取决于选定的密钥长度。

利用 RSA 公开密钥算法在密钥自动管理、数字签名、身份识别等方面的特性,可建立一个为用户的公开密钥提供担保的可信的第三方认证系统。这个可信的第三方认证系统也称为 CA,CA 为用户发放电子证书,用户之间(比如网银服务器和某客户之间)利用证书来保证信息安全性和双方身份的合法性。

2) 系统结构

核心系统和 CA 放在一个单独的封闭空间中,为了保证运行的绝对安全,其人员及制度都应有严格的规定,并且系统设计为离线网络。CA 的功能是在收到来自 RA 的证书请求时颁发证书。一般的个人证书发放过程都是自动进行,无须人工干预。

证书的登记机构(register authority,RA)分散在各个网上银行的地区中心。RA 与网银中心有机结合,接受客户申请,并审批申请,把证书正式请求通过银行企业内部网发送给 CA 中心。RA 与 CA 双方的通信报文也通过 RSA 进行加密,确保安全。系统的分布式结构适于新业务网点的开设,具有较好的扩充性。通信协议为 TCP/IP。

证书的公布系统(Web publisher,WP)置于 Internet 上,是普通用户和 CA 直接交流的界面。对用户来讲它相当于一个在线的证书数据库。用户的证书颁发之后,CA 用 E-mail 通知用户,然后用户须用浏览器从这里下载证书。

### 2. SSL 协议

SSL 协议是 Netscape 公司在网络传输层上提供的一种基于 RSA 和保密密钥的用于浏览器和 Web 服务器之间的安全连接技术。它被视为 Internet 上 Web 浏览器和服务器的标准安全性措施。SSL 提供了用于启动 TCP/IP 连接的安全性“信号交换”。这种信号交换导致客户和服务器同意将使用的安全性级别,并履行连接的任何身份验证要求。它通过数字签名和数字证书实现浏览器和 Web 服务器双方的身份验证。在用数字证书对双方的身份验证后,双方就可以用保密密钥进行安全会话了。

SSL 协议在应用层收发数据前,协商加密算法、连接密钥并认证通信双方,从而为应用层提供了安全的传输通道。在该通道上可透明加载任何高层应用协议(如 HTTP、FTP、TELNET 等)以保证应用层数据传输的安全性。SSL 协议独立于应用层协议,因此在电子交易中被用来安全传送信用卡号码。

中国目前多家银行均采用 SSL 协议,如在目前中国的电子商务系统中能完成实时支付,用的最多的招行一网通采用的就是 SSL 协议。所以,从目前实际使用的情况看,SSL

还是人们最信赖的协议。

SSL 当初并不是为支持电子商务而设计的,所以,在电子商务系统的应用中还存在很多弊端。它是一个面向连接的协议,在涉及多方的电子交易中,只能提供交易中客户与服务器间的双方认证,而电子商务往往是用户、网站、银行三家协作完成,SSL 协议并不能协调各方间的安全传输和信任关系。还有,购货时用户要输入通信地址,这样可能使得用户收到大量垃圾信件。

因此,为了实现更加完善的电子交易,MasterCard 和 Visa 以及其他一些业界厂商制定并发布了 SET 协议。

### 3. SET 协议

SET 协议是针对开放网络上安全、有效的银行卡交易,由 Visa 和 MasterCard 联合研制的,为 Internet 上卡支付交易提供高层的安全和反欺诈保证。

SET 协议保证了电子交易的机密性、数据完整性、身份的合法性和抗否认性。

SET 是专门为电子商务而设计的协议,虽然它在很多方面优于 SSL 协议,但仍然不能解决电子商务所遇到的全部问题。而且,SET 遭到有些银行的抵制,其前途如何,尚未得知。

### 4. SSL 协议与 SET 协议的比较

1) SSL 的优势与劣势

SSL 是一个比较成熟的通信传输协议。由于 SSL 已嵌入 Web 浏览器和服务器,使用方便,因此得到广泛应用。而且它对应用层来说是透明的,不需要修改应用程序,这给用户带来了很大的便利。网上银行、支付系统在传输机密数据时,经常使用 SSL 协议。另一方面,SSL 协议并非专门为电子商务设计,它负责端到端的安全连接,只保证信息传输过程中不被盗取、篡改,但不提供其他安全保证。防止客户抵赖的一种方法是向持卡人颁发数字证书,以鉴别客户的真实身份。这样,基于 SSL 的安全协议又向 SET 靠近了一步。另一种方法是采用“表单签名”,利用这一功能对应用层消息进行数字签名,从而弥补 SSL 缺乏数字签名和不可否认性的缺陷。

另外,对中国用户来说,SSL 协议的一个严重缺陷就是加密强度太弱,因为美国政府限制,所以出口到我国的 SSL 的密钥长度仅有 40 位。

2) SET 的优势与劣势

SET 协议的最明显特征是通过 CA 认证体系,建立交易各方的信任关系。它不仅具有加密机制,更重要的是通过数字签名、数字信封等实现身份鉴别和不可否认性。SET 对商家尤其是客户提供了更加周到的安全保护,最大限度地降低遭受欺诈的风险。SET 规范了电子商务活动的流程,即规范了从持卡人到商家、到支付网关、到认证中心及银行之间的信息流向和严密的加密、认证标准。SET 的“双重签名”机制能够最大限度地保护消费者的利益。SET 对软硬件环境要求较高,交易成本较高。首先,SET 交易是基于信用卡的,因此,它面向的是社会中的一部分群体——持卡族;其次,要有一个权威的认证中心(CA)审核并颁发各种电子证书,包括持卡人证书、特约商户证书、支付网关证书收

单行证书和发卡行证书；最后，在银行、商家和客户端分别要安装专门的软件，比如客户端的电子钱包软件用于完成身份鉴别、加密、数字签名等一系列工作。为了安全存放私钥及证书客户最好拥有智能卡、读卡器等设备。目前流行的一种方案就是所谓“面向商家的 SET”即银行与商家之间使用 SET，而商家与客户之间仍使用 SSL，这种方案回避了客户端安装电子钱包软件，但没有彻底解决客户容易遭受欺诈的问题。

#### 5. 与电子商务安全有关的其他技术

1）密码技术

密码技术基本思想是在加密密钥 Ke 的控制下按照加密算法 E 对要保护的数据（即明文 M）加密成密文 C，记为 C＝E(M，Ke)。而解密是在解密密钥 Kd 的控制下按照解密算法 D 对密文 C 进行反变换后还原为明文 M，记为 M＝D(C，Kd)。根据密钥性质的不同，可分为传统密码体制和公开钥密码体制两大类型。密码技术是上面所提到的几种技术的基础，所以，可以说整个电子商务的安全就是建立在密码技术基础上的。

2）访问控制

除了计算机网络硬件设备之外，网络操作系统是确保计算机网络安全的最基本部件。它是计算机网络资源的管理者，必须具备安全的控制策略和保护机制，防止非法入侵者攻破设防而非法获取资源。网络操作系统安全保密的核心是访问控制，即确保主体对客体的访问只能是授权的，未经授权的访问是不允许的，其操作是无效的。因此，授权策略和机制的安全性显得特别重要。保护可以从物理隔离、时间隔离、密码隔离几个方面加以考虑。

3）防火墙技术

设立防火墙的目的是保护内部网络不受外部网络的攻击，以及防止内部网络的用户向外泄密。目前，防火墙技术主要是分组过滤和代理服务两种类型。分组过滤是一种基于路由器的防火墙。它是在网间的路由器中按网络安全策略设置一张访问表或黑名单，即借助数据分组中的 IP 地址确定什么类型的信息允许通过防火墙，什么类型的信息不允许通过。目前，80％的防火墙都是采用这种技术。代理服务是一种基于代理服务的防火墙，它的安全性高，增加了身份认证与审计跟踪功能，但速度较慢。

4）数字时间戳

交易文件中，时间是十分重要的信息。在书面合同中，文件签署的日期和签名一样均是十分重要的防止文件被伪造和篡改的关键性内容。在电子交易中，同样需对交易文件的日期和时间信息采取安全措施，而数字时间戳服务（digital time-stamp service，DTS）就能提供电子文件发表时间的安全保护。

DTS 是网上安全服务项目，由专门的机构提供。时间戳（time-stamp）是一个经加密后形成的凭证文档，它包括需加时间戳的文件的摘要（digest）、DTS 收到文件的日期时间和 DTS 的数字签名。

#### 6. 企业实现电子商务的安全策略

安全问题是企业应用电子商务最担心的问题，如何保障电子商务活动的安全，一直

是电子商务的核心研究领域。作为一个安全的电子商务系统,必须采用相应的网络安全策略。安全策略包括网络安全问题的总原则、对安全使用的要求以及如何保障网络的安全运行。

1) 制定安全策略时首先确定的最重要的原则

当前一些电子商务企业的安全策略存在两个误区:首先,企业所采取的操作系统的标准安全策略存在问题。这一标准安全策略只能提供一道脆弱的防线,很容易被攻破。其次,为满足多种安全需求,许多企业以零碎的方式实施节点式解决方案,这虽然对电子商务的某些领域提供了有限的保护,但同时使系统管理更为复杂。阻止外来系统入侵只是电子商务安全的一个方面。成功的电子商务安全策略,必须涵盖身份识别与认证、隐私与欺骗控制、管理与审计等传统领域。

2) 安全策略制定时还应注意的问题

① 将需要保护的对象分类,确定需要保护的资源及其保护级别。规定可以访问资源的实体和可执行的动作。规定审计功能,记录用户活动及资源使用情况。

② 系统的安全应从物理上、技术上、管理制度上以及安全教育上全方位采取措施,相互弥补和完善,尽可能地排除安全漏洞。

③ 根据企业的实际需要确定内部网的服务类型,规定内部用户和外部用户能够使用的服务种类,建立网管站,并制定出切实可行的安全管理制度。此外还需完善电子商务企业内部安全管理体制,增强相关人员的安全意识。

## 习 题 5

(1) 简述 SMTP 协议的连接和发送过程、路由过程。

(2) 简述 POP3 协议的工作原理。

(3) 综述电子邮件安全策略。

(4) 简述 Windows IIS 安全设置,并以实例说明。

(5) 简述制定 Web 站点安全策略的原则。

(6) 简述 Web 服务器安全漏洞的消除方法。

(7) 简述企业信息化建设的安全隐患。

(8) 综述电子商务的安全策略。

# 第 6 章 chapter 6

# 黑客防范技术

随着互联网的规模不断扩大以及人类社会对网络的依赖程度越来越大，在开放的网络环境下，有越来越多的非法用户利用黑客技术频繁攻击网络，网络安全问题日益突出，已经成为危害人们的日常生活和社会发展的重要因素。例如，远程办公室或分支办公室在中小企业十分盛行，在发达地区有 40%～50%的员工采用上述工作形式。员工可以在公司以外使用手机、智能电话、笔记本计算机等不同设备随时存取公司网络的业务信息。黑客可以伺机破坏，造成身份盗窃及资料外泄等问题。加上大部分中小企业通常只会使用一个服务器作中枢，负责整体网络运作，一旦系统被入侵，黑客可以任意盗取，甚至更改企业重要资料，令公司在经济上、声誉上均蒙受损失。另外，目前广泛使用即时信息、社交网站、影片分享平台等应用，会直接危害企业的网络安全。黑客会在上述网站内大肆搜寻网民数据，然后寻找攻击对象。假如企业员工在办公室内浏览了以上网页，公司网络可能会成为僵尸网络(Bot)，在不知情的情况下发送数以百万计的垃圾电子邮件，或是被植入键盘记录(Keylogger)程序，窃取密码，造成经济上的损失。

因此，为了维护计算机网络和信息的安全，给用户提供一个安全的网络应用环境，需要认真研究黑客技术，分析黑客入侵及攻击原理，以便寻找出对策。本章将向读者介绍目前黑客经常采用的攻击技术以及防范黑客的技术手段和一些实用的防范黑客的常识。

## 6.1 黑客概述

### 6.1.1 黑客类型

“黑客”大体上应该分为“正”、“邪”两类，正派黑客依靠自己掌握的知识帮助系统管理员找出系统中的漏洞并加以完善，而邪派黑客则是通过各种黑客技能对系统进行攻击、入侵或者做其他一些有害于网络的事情，因为邪派黑客所从事的事情违背了《黑客守则》，所以他们真正的名字叫“骇客”(cracker)而非“黑客”(hacker)，也就是平时常听说的“黑客”和“红客”。

黑客通常可以分为以下几种类型。

#### 1. 好奇型

这类黑客喜欢追求技术上的精进，只在好奇心驱使下进行一些并无恶意的攻击，以

不正当侵入为手段找出网络漏洞，一旦发现了某些内部网络漏洞后，会主动向网络管理员指出或者干脆帮助修补网络错误以防止损失扩大，使网络更趋于完善和安全。

#### 2. 恶作剧型

这类黑客的数量也许是最多最常见的。他们闯入他人网站，以篡改、更换网站信息或者删除该网站的全部内容，并在被攻击的网站上公布自己的绰号，以便在技术上寻求刺激，炫耀自己的网络攻击能力。

#### 3. 隐匿型

这类黑客喜欢先通过种种手段把自己深深地隐藏起来，然后再以匿名身份从暗处实施主动网络攻击。有时干脆冒充网络合法用户，通过正常渠道侵入网络后再进行攻击。他们大都技术高超、行踪无定，攻击性比较强。

#### 4. 定时攻击型

这是极具破坏性的一种类型。为了达到某种个人目的，黑客通过在网络上设置陷阱或事先在生产或网络维护软件内置入逻辑炸弹或后门程序，在特定的时间或特定条件下，根据需要干扰网络正常运行或导致生产线或网络完全陷入瘫痪状态。

目前，黑客的本质正在发生明显的改变。他们已经从独立个体演变为有共同目标并合作出击的“黑客群”。而黑客的目标也由只求成名变成以金钱为目标，这个转变令黑客的行为大受影响，以致他们不再以破坏为主导，反而利用系统漏洞，在用户不知情之下，盗取企业机密、网上银行密码等重要资料。现在黑客则主要依靠远程攻击，一则针对服务器，寻找对方程序漏洞，进行侵入，既而蔓延对方网络；另一则是针对个人用户，远程植入木马程序。“技术好的黑客所用的木马程序，都是定制的，一般病毒软件和防火墙都不会有反应。”

今后，网络罪犯们会逐渐将重点放在攻击那些有可能获利丰厚的目标上，他们不大可能掀起大规模网络病毒攻击的浪潮，而是每次只攻击一到两个公司，但是相应的回报却可能是巨大的。利用“特洛伊木马”的计算机程序来复制窃取许多国家的顶级商业公司的机密信息，已经变得越来越频繁。定向木马攻击的程序编写者只针对少数几个公司编写和使用某种特殊的木马。他们发起的攻击规模通常都很小，很容易就躲开了网络安全公司的监视，因为网络安全公司都在寻找较大规模的攻击。

### 6.1.2 黑客的行为特征

无论哪类黑客，他们最初的学习内容都将是本部分所涉及的内容，而且掌握的基本技能也都是一样的。即便日后他们各自走上了不同的道路，但是所做的事情也差不多，只不过出发点和目的不一样而已。黑客的行为主要有以下几种。

#### 1. 学习技术

互联网上的新技术一旦出现，黑客就必须立刻学习，并用最短的时间掌握这项技术，

这里所说的掌握并不是一般的了解，而是阅读有关的“协议”(rfc)、深入了解此技术的机理。否则一旦停止学习，那么依靠他以前掌握的内容，并不能维持他的“黑客”身份超过一年。

初级黑客要学习的知识是比较困难的，因为他们没有基础，所以学习起来要接触非常多的基本内容，然而今天的互联网给读者带来了很多的信息，这就需要初级学习者进行选择，太深的内容可能会给学习带来困难，太“花哨”的内容又对学习黑客没有用处。所以初学者不能贪多，应该尽量寻找一本书适合自己的完整教材，循序渐进地进行学习。

**2. 伪装自己**

黑客的一举一动都会被服务器记录下来，所以黑客必须伪装自己使得对方无法辨别其真实身份，这需要有熟练的技巧，用来伪装自己的 IP 地址、使用跳板逃避跟踪、清理记录扰乱对方线索、巧妙躲开防火墙等。

伪装是需要非常过硬的基本功才能实现的，这对于初学者来说称得上“大成境界”了，也就是说初学者不可能用短时间学会伪装，所以并不鼓励初学者利用自己学习的知识对网络进行攻击，否则一旦自己的行迹败露，最终受害的是自己。

真正的黑客，同样不赞成对网络进行攻击，因为黑客的成长是一种学习，而不是一种犯罪。

**3. 发现漏洞**

漏洞对黑客来说是最重要的信息，黑客要经常学习别人发现的漏洞，并努力自己寻找未知漏洞，并从海量的漏洞中寻找有价值的、可被利用的漏洞进行试验，当然他们最终的目的是通过漏洞进行破坏或者修补上这个漏洞。

黑客对寻找漏洞的执著是常人难以想象的，他们的口号是“打破权威”，从一次又一次的黑客实践中，黑客也用自己的实际行动向世人印证了世界上没有“不存在漏洞”的程序。在黑客眼中，所谓的“天衣无缝”不过是“没有找到”而已。

**4. 利用漏洞**

对于正派黑客来说，漏洞要被修补。对于邪派黑客来说，漏洞要用来搞破坏。而他们的基本前提是“利用漏洞”，黑客利用漏洞可以做下面的事情。

(1) 获得系统信息：有些漏洞可以泄露系统信息，暴露敏感资料，从而进一步入侵系统。

(2) 入侵系统：通过漏洞进入系统内部，或取得服务器上的内部资料，或完全掌管服务器。

(3) 寻找其他入侵目标：黑客充分利用自己已经掌管的服务器作为工具，寻找并入侵其他目标系统。

(4) 做一些好事：正派黑客在完成上面的工作后，就会修复漏洞或者通知系统管理员，做出一些维护网络安全的事情。

(5) 做一些坏事：邪派黑客在完成上面的工作后，会判断服务器是否还有利用价值。

如果有利用价值,他们会在服务器上植入木马或者后门,便于下一次来访。而对没有利用价值的服务器他们绝不留情,系统崩溃会让他们产生无限的快感!

为了反追踪和隐身,现在的黑客还往往采用第三方攻击,即选取跨地区或跨国界的第三方个人 PC 或服务器作为跳板,一旦对方跟踪,几乎不可能追溯到攻击的最终来源。

目前还出现了越来越多的释放特洛伊木马的自动工具以及其他入侵复杂系统的工具,它们非常快地沿“食物链”升级。窃取信息正在成为木马的主要目的。现在的趋势是,病毒开始集中进攻特定的组织,并试图种木马。因此,提高安全防范意识,建立起综合的网络安全监控防御体系,及时下载操作系统和应用程序的补丁,堵住存在的漏洞将是十分必要的。

### 6.1.3 黑客攻击的目的

一般情况下,黑客的攻击总有明确的目的性。由于黑客们成长的经历和生活工作环境不同,其攻击目标也会多种多样,但大致上可以归纳总结如下。

#### 1. 窃取信息

黑客攻击最直接的目标就是窃取信息。黑客选取的攻击目标往往是重要的信息和数据,在获得这些信息与数据之后,黑客就可以进行各种犯罪活动。政府、军事、邮电和金融网络是黑客攻击的首选目标。随着计算机与网络技术在政府、军事、金融、医疗、交通及电子等各个领域的广泛应用,黑客的各种破坏活动也随之猖獗。

窃取信息包括破坏信息的保密性和完整性。破坏信息的保密性是指黑客将窃取到的需要保密的信息发往公开的站点。而破坏信息的完整性是指黑客对重要文件进行修改、更换和删除,使得原来的信息发生了变化,以至于不真实或者错误的信息给用户带来难以估量的损失。

#### 2. 获取密码

事实上,获取密码也是窃取信息的一种,由于密码的特殊性,所以单独列出。黑客通过登录目标主机,或使用网络监听程序进行攻击。监听到密码后,便可以顺利地登录到其他主机,或者去访问一些本来无权访问的资源。

#### 3. 控制中间站点

在某些情况下,黑客登上目标主机后,不是为了窃取信息,只是运行一些程序,这些程序可能是无害的,仅仅消耗一些系统的处理时间。比如,黑客为了攻击一台主机,往往需要一个中间站点,以免暴露自己的真实所在。这样即使被发现,也只能找到中间站点的地址,而真正的攻击者可以隐藏起来。再比如,黑客不能直接访问某一严格受控制的站点或网络,此时就需要一个具有访问权限的中间站点,所以这个中间站点就成为了首先要攻击的目标。

#### 4. 获得超级用户权限

黑客在攻击某一个系统时，都企图得到超级用户权限，这样就可以完全隐藏自己的行踪，并可在系统中埋伏下方便的后门，便于修改资源配置，做任何只有超级用户才能做的事情。

### 6.1.4 黑客攻击的过程

通常，黑客攻击所采用的技术和手段可能不同，攻击目标也可能不同，但黑客进行网络攻击时都遵循一定的规律，其过程大致是一样的，一般可以分为攻击前奏、实施攻击、巩固控制、深入攻击和扫除痕迹等几个过程。

从理论上讲没有一个系统是绝对安全的，除非这个系统和外界没有任何的联系，没有输入，也没有输出。所有的攻击是建立在上面的这条大原则下的。只要系统和外界有交互，那就能攻击进去。如果存在系统漏洞的话，攻击会变得更加简单。下面讲一下攻击的大致步骤和所用到的技术。

#### 1. 确定目标

黑客进行攻击，首先要确定攻击目标。比如，某个具有特殊意义的站点、某个有利可图的 ISP、一些金融银行网站、具有敌对观点的宣传站点或解雇了黑客的单位主页等。

#### 2. 收集目标计算机的信息

黑客收集欲攻击的计算机的所有相关信息，这些信息包括目标计算机的软、硬件信息（如操作系统、用户信息、驻留在网络系统中的各个主机系统的相关信息等），运行的操作系统信息运行的应用程序（服务）的信息，目标计算机所在网络的信息。常见的信息收集方法包括在域名及其注册机构的查询，对公司性质的了解，对主页进行分析，邮件地址的搜集，目标 IP 地址范围查询。

黑客认为，只要系统与 Internet 连接，他们就能够找到漏洞，因为网络中的漏洞太多了，从操作系统、网络服务到网络协议，还有缓存区都存在漏洞。据全球最大的防黑客软件公司 ISS 公司的创始人 Claus 说，目前他们已经掌握了至少 5000 多个漏洞。在收集到攻击目标的相关信息之后，黑客分析探测网络上的每台主机，以寻求该系统的安全漏洞和安全弱点。

信息收集的目的就是探察对方的各方面情况，寻找系统的安全漏洞，摸清楚对方最薄弱的环节和守卫最松散的时刻，确定攻击的时机，为下一步的入侵提供良好的策略，比如可以通过以下网络地址很方便地获取目标服务器的信息。

中国互联网络信息中心：www. nic. com/nic_info/whois. htm、www. nic. com/cgi_bin/whois. cgi。

中国万网域名服务系统：www. net. cn/domain。

黑客会利用下列公开的协议或工具，收集驻留在网络系统中的各个主机系统的相关信息。

(1) SNMP 协议,用于查阅网络系统路由器的路由数,从而了解目标主机所在网络的拓扑结构及其内部细节。

(2) Tracert 程序,用于获得到达目标主机所要经过的网络数和路由器数。

(3) Whois 协议,利用该协议的服务信息可获得所有有关 DNS 域和相关的管理参数。

(4) DNS 服务器,提供了系统中可以访问的主机的 IP 地址表和它们所对应的主机名。

(5) Finger 协议,用于获取一个指定主机上的所有用户的详细信息(如用户注册名、最后注册时间以及他们是否读邮件等)。

(6) ping 实用程序,用于确定一个指定主机的位置。

(7) 自动 Wardialing 软件,用于向目标站点一次连续拨出大批电话号码,直到遇到某一正确的号码使其 Modem 响应。

(8) 自编程序,如果某些产品或者系统已经发现了一些安全漏洞,该产品或系统的厂商或组织会提供一些“补丁”程序来弥补。但是若用户没有及时打上“补丁”,黑客会利用这些漏洞来自己编写程序进入目标系统。

(9) 在网络系统中,为了帮助系统管理员发现其管理的网络系统内部隐藏的安全漏洞,完善系统并堵塞漏洞,一些网络公司编制了一些网络扫描、分析、检测的工具软件。黑客也常常利用这些工具得到目标系统的信息,获取攻击目标系统的非法访问权。比如 ISS(interact security scanner)、SATAN(security analysis toolfor auditing network)等,这样的工具可以对整个网络或子网进行扫描,寻找安全漏洞。这样的工具既可被网络安全管理员用来作为检测网络安全性的有力武器,也可以被黑客用来作为扫描网络漏洞的黑客工具。类似的收集信息工具有 Visualroute、AdvancedProperies、Smartwhois、Sam spade、Netscantoos 等,命令行方式手机信息的工具有 Finger、Whois、Nalookup、Dig、Tracert、Tracerroute 等。

### 3. 寻找目标计算机的漏洞和选择合适的入侵方法

黑客分析所得到的攻击目标的信息,找到安全的漏洞和弱点,然后选择合适的攻击方法,如破解密码、缓存区溢出攻击、拒绝服务攻击、IP 电子欺骗等,其目的是进入系统并获得系统的控制权限。这里主要有两种方法通过发现目标计算机的漏洞进入系统或者是利用密码猜测进入系统。利用密码猜测就是试图重复登录,直到找到一个合法的登录为止。这种方法往往会消耗大量的时间,而且每次登录不管是否成功都会在目标计算机上留下记录,会引起注意。另一个就是利用和发现目标计算机的漏洞,直接顺利进入。

发现目标计算机漏洞的方法用得最多的就是缓存区溢出法。通过这个方法,使得目标计算机以最高级别的权限来运行攻击者设定的后门程序,从而进入系统。发现系统漏洞的第二个方法就是平时参加一些网络安全列表。在全球有关网络安全列表里,经常有最新发现的系统或应用程序的漏洞的公告。然后根据第一步扫描系统得到的信息来看看是否有漏洞可以利用。

还有一些入侵的方法是采用 IP 地址欺骗等手段。它的原理就是通过各种欺骗手段，取得目标计算机的信任从而可以进入目标计算机。

黑客一旦获得了对攻击目标系统的访问权后，可以有以下多种选择。

（1）可能试图毁掉攻击入侵的痕迹，并在系统中建立另外的新的安全漏洞和后门，以便先前的攻击点被发现后，继续访问系统。

（2）可能在目标系统中安装探测器软件，包括特洛伊木马程序，用来窥探所在系统的活动，收集黑客感兴趣的一切信息。

（3）可能进一步发现受损系统在网络中的信任等级，然后进一步通过该中间系统展开对整个系统的攻击。

（4）若黑客在受损系统上获得了特许访问权，就可以读取邮件、搜索和盗窃私人文件以及毁坏重要数据，从而破坏整个系统的信息，造成不堪设想的后果。

（5）黑客在攻击得手后，往往会继续在系统中寻找相关主机的可用信息，从而攻击其他系统。

#### 4. 留下“后门”

黑客根据收集或探测到的信息，在选择合适的方法后，黑客就会侵入到系统中，但这只是攻击的前奏。黑客如果进一步发现受害系统在网络中的信任等级，那么就可以通过该系统信任级展开对这个系统的攻击。如果该黑客在这台受害系统上获得了特许访问权，那么他就可以读取邮件、搜索和盗窃私人文件、毁坏重要数据，破坏整个系统的信息，从而造成不堪设想的后果。

在侵入目标计算机后留下后门的目的是为以后进入该系统提供方便。一般是在受到侵害的系统上找到另外的新的漏洞或留下“后门”，并安装探测软件，其中包括特洛伊木马程序，用来窥测所在系统的活动，收集进一步感兴趣的信息，如 Telnet 和 FTP 的用户名和密码等。它在系统运行的同时运行，而且能在系统以后的重新启动时自动运行这个程序。

#### 5. 清除入侵记录

清除入侵记录是把在入侵系统时的各种登录信息都删除，以防被目标系统的管理员发现，以便能够继续访问这个系统。继续收集信息应该是入侵系统的目的。采取的手法很多，例如，通过 sniffer 程序来收集目标系统网络的重要数据。还可以通过后门，即一个特洛伊木马程序收集信息，例如，发送一个文件复制命令，把目标计算机上的有用文件复制过来。

由于入侵的目标计算机可能运行的操作系统、应用程序很多。因此，没有一种固定的入侵方法。这往往要求攻击者具有丰富的计算机和网络方面的知识，特别是需要网络编程方面的知识和操作系统高级编程知识。只要知道一些网络安全技术方面的基础知识，再加上一些编程知识，根据不同的操作系统，就能成功地实施对目标计算机系统的攻击了。

### 6.1.5 黑客攻击方式

计算机黑客对网络系统的攻击方法以及所使用的工具也正向智能化、网络化发展，并已出现了一些利用网络最新技术的智能化工具软件。由于黑客技术在网上交流的充分性，我国黑客应用的技术手段，与国外黑客大致相同。按攻击距离划分，黑客攻击的方式有以下两种。

**1. 远程攻击**

指外部黑客通过各种手段，从该子网以外的地方向该子网或者该子网内的系统发动攻击。远程攻击的时间一般发生在目标系统当地时间的晚上或者凌晨时分，因为此时网速较快，网络管理也较松懈，攻击不容易发现。远程攻击发起者一般不会用自己的机器直接发动攻击，而是通过跳板的方式，对目标进行迂回攻击，以迷惑系统管理员，防止暴露真实身份。

**2. 本地攻击**

本地攻击指本单位的内部人员通过所在的局域网，向本单位的其他系统发动攻击。在本机上进行非法越权访问也是本地攻击。还有一种叫伪远程攻击，它是指内部人员为了掩盖攻击者的身份，从本地获取目标的一些必要信息后，攻击过程从外部远程发起，造成外部入侵的现象，从而使追查者误认为攻击者是来自外单位。

另外，根据黑客对所攻击系统的破坏程度，分为以下两类。

1）主动攻击

这种攻击以各种方式获取攻击目标的相关信息，找出系统漏洞，侵入系统后，将会有选择地破坏信息的有效性和完整性，如邮件炸弹。

2）被动攻击

这种攻击是在不影响网络正常工作的情况下，进行监听、截获、窃取、破译以获得重要机密信息，其中包括窃听和通信流量分析。例如，利用 Sniffer Pro 网络监听工具就可以对网络进行监听，并进行协议分析。

## 6.2 网络攻击的技术手段

“知己知彼，百战不殆”，要想有效防御黑客攻击，必须对敌人的武器和作战手段耳熟能详。作为一个优秀的网络安全专家，除了精通网络防御之外，还要做一个比黑客更“黑”的“黑客”。

### 6.2.1 网络攻击分类

只要系统连接到网络上，就有可能受到攻击。对于不同的系统，存在的漏洞不同，攻击的方法也不相同。一般来讲，攻击总是利用“系统配置的缺陷”、“操作系统的安全漏洞”或“通信协议的安全漏洞”来进行的。到目前为止，已经发现的攻击方式超过 2000

种，大概可以划分为以下六类。

（1）拒绝服务攻击。一般情况下，拒绝服务攻击是通过使被攻击对象的系统关键资源过载，从而使被攻击对象停止部分或全部服务。目前已知的拒绝服务攻击就有几百种，它是最基本的入侵攻击手段，也是最难对付的入侵攻击之一。典型示例有 SYN Flood 攻击、ping Flood 攻击、Land 攻击、WinNuke 攻击等。

（2）非授权访问尝试是攻击者对被保护文件进行读、写或执行的尝试，也包括为获得被保护访问权限所做的尝试。

（3）预探测攻击。在连续的非授权访问尝试过程中，攻击者为了获得网络内部的信息及网络周围的信息，通常使用这种攻击尝试。典型示例包括 SATAN 扫描、端口扫描和 IP 半途扫描等。

（4）可疑活动。是通常定义的“标准”网络通信范畴之外的活动，也可以指网络上不希望有的活动，如 IP Unknown Protocol 和 Duplicate IP Address 事件等。

（5）协议解码。协议解码可用于以上任何一种非期望的方法中，网络或安全管理员需要进行解码工作，并获得相应的结果。解码后的协议信息可能表明期望的活动，如 FTU User 和 PortmapperProxy 等解码方式。

（6）系统代理攻击。这种攻击通常是针对单个主机发起的，而并非整个网络，通过 RealSecure 系统代理可以对它们进行监视。

对上述的攻击根据攻击的性质、严重程度、攻击目标，可以进行不同的分类。按照攻击的性质，通常可以分成保守型（passive attack）攻击即被动攻击和进攻型（aggressive attack）攻击即主动攻击。下面通过两个例子来说明保守攻击型和进攻型攻击的不同。

例如，甲是一个顾客，乙是一家银行，甲从网络上查询信用卡的余额并进行转账。在进行这些操作之前，甲首先要输入信用卡的账号和密码之后，在账号和密码通过网络传输银行主机的过程中，丙从网络上窃取这些信息。但丙并没有干扰甲的操作，甲也不知道丙在窃取他的信息，甲按照正常的操作，完成他所要做的事情，并退出了网络。这种不影响正常通信的攻击手段，叫做保守型攻击，它影响的是数据的保密性（Confidentiality）。丙可以利用窃取来的信息，伪造另一张相同号码的信用卡去支付消费，把甲的钱都花个精光，也能对甲造成利益上的损害。

黑客要进行保守型攻击，需要一些条件。基本来讲，要能在物理上接近数据传输的通道。无论是溜进计算机房、在键盘上方装个针孔摄像机、在房间外安装无线电接收器接收计算机辐射出来的信息、偷偷切入电话线或网线，还是通过无线电窃听移动设备。最常见的，应该是在数据传输通道中间窃取。如果信号的传输方式是按照基带方式进行传输的，窃取这些数据是非常方便的。如果将数据进行了调制，特别是时分多址（TDMA）和码分多址（CDMA）方式复用，将数据按一定的方式进行了变换，窃取数据会困难一些。当然，后面还会讲到，利用特洛伊木马程序也可以窃取这些数据。

最容易得到其他用户数据的环境，莫过于局域网了。众所周知，计算机是通过网卡连接到局域网的，目前广泛使用的以太网卡有固定的物理地址，也叫做 MAC 地址，这个地址是全球唯一的（有些网卡的地址可以自己设定）。大多数的网卡都有两种工作模式，普通模式和混杂模式（promiscuous mode）。正常情况下，网卡都被设置在普通模式，当检测到网络上有数据帧到达时，网卡通常会检查数据帧的目的地址，如果该地址和本卡

的地址相符，就向网络的上层传递这个数据帧；如果该地址和自己的地址不同时，就会把这个帧丢掉。当网卡工作在混杂模式时，接口不再检查所接收到的数据帧的目的地址，而是直接把数据帧接收下来，传递给网络的上层。只要是完整的数据帧就会被传递上去，这样配置的所有用户只要能连接到局域网，就能读取网上传输的数据。

再来看另外一种情况。假如丙仿造了银行的计算机系统，并欺骗了甲的DNS系统，甲在输入银行的域名地址并开始连接后，甲的计算机没有连接到真正的银行计算机系统，而是连接到丙的计算机系统，丙的计算机系统接受了甲传来的信息"转账￥1000到另一个账户××××"，并把这些信息变成"转账￥1000到另一账户××××，并转账￥100元到丙的账户××××"。在这种攻击中，丙恶意篡改了甲和乙之间传输的数据，不但影响了数据的保密性，而且影响了数据的完整性以及数据的真实性，通常把它叫做进攻型攻击。

2005年爆发的"网络钓鱼"攻击就是典型的进攻型攻击，它利用欺骗性的电子邮件和伪造的Web站点来进行诈骗活动，受骗者往往会泄露自己的财务数据，如信用卡号、账户用户名、密码和社保编号等内容。诈骗者通常会将自己伪装成知名银行、在线零售商和信用卡公司等可信的品牌。在所有接触诈骗信息的用户中，有高达5%的人都会对这些骗局做出响应。

由此可以看到，这两种攻击手段并不是截然分开的。如果甲是银行的网络管理员，丙从网络上窃取了甲的账号和密码，甚至窃取了超级用户的密码，他就可以利用这些账号和密码，进入银行的计算机系统，肆意地删除和篡改数据，把银行的资金转到其他的账户。然后，从这些账户支取现金进行消费。也就是说，黑客可以利用保守型攻击得到的信息，进行进攻型攻击。保守型攻击成为进攻型攻击的基础。

实际上，对于现在的Internet来讲，还有一种类型的攻击方式，既不破坏数据的保密性，也不破坏数据的完整性，而是采用各种手段让客户机无法和服务器进行连接，即服务器不能为客户机提供服务。这种攻击方式就是广为所知的拒绝服务（Dial of Service），通常简称为DoS攻击。

因此，黑客的攻击造成的后果包括破坏数据的完整性、数据的保密性、数据的真实性以及服务器拒绝服务。可以总结一下，把攻击方式归类为表6-1所示。

**表6-1 黑客攻击的手段及其后果**

| | 完整性 | 保密性 | 真实性 | 拒绝服务 |
|---|---|---|---|---|
| 威胁 | • 篡改用户数据<br>• 特洛伊木马<br>• 修改内存<br>• 修改传输过程中的数据 | • 网络窃听<br>• 盗窃服务器信息<br>• 盗窃客户端信息<br>• 盗窃网络配置信息<br>• 盗窃客户和服务器交流的信息 | • 冒充合法用户<br>• 伪造数据 | • 杀死用户进程<br>• 用假请求轰炸系统<br>• 把硬盘或内存占满<br>• 用DoS攻击孤立系统 |
| 结果 | 丢失信息<br>系统破坏<br>容易受到其他攻击 | 丢失信息<br>暴露隐私 | 错误的用户<br>接收假信息 | 破坏<br>烦恼<br>用户无法完成工作 |
| 措施 | 加密验证 | 加密 | 加密技术 | 很难防止 |

### 6.2.2 端口扫描与漏洞攻击

许多网络入侵是从扫描开始的。利用扫描工具能找出目标主机上各种各样的漏洞来,有些漏洞尽管早已公布于众,但在一些系统中仍然存在,于是给了外部入侵可乘之机。常用的短小而实用的端口扫描工具是一种获取主机信息的好方法。在 UNIX 系统中,使用端口扫描程序不需要超级用户权限,任何用户都可以使用。而且简单的端口扫描程序非常容易编写,掌握了初步的 Socket 编程知识,便可以轻而易举地编写出能够在 UNIX 和 Windows NT 下运行的端口扫描程序。黑客们常常用扫描工具找出系统漏洞或者是主机信息,然后展开攻击。

**1. 网络扫描概述**

网络扫描一般分成两种策略,被动式策略和主动式策略。被动式策略是基于主机之上,对系统中不合适的设置、脆弱的密码以及其他同安全规则抵触的对象进行检查。主动式策略是基于网络,它通过执行一些脚本文件模拟对系统进行攻击的行为并记录系统的反应,从而发现其中的漏洞。扫描的目的是利用各种工具对攻击目标的 IP 地址或地址段的主机查找漏洞。扫描采取模拟攻击的形式对目标可能存在的已知安全漏洞逐项进行检查,目标可以是工作站、服务器、交换机、路由器和数据库应用等。根据扫描结果向扫描者或管理员提供周密可靠的分析报告。

(1) 主动策略扫描。主动式扫描一般可以分成:活动主机探测;ICMP 查询;网络 ping 扫描;端口扫描;标识 UDP 和 TCP 服务;指定漏洞扫描;综合扫描等。

扫描方式可以分成两大类,慢速扫描和乱序扫描。慢速扫描是对非连续端口进行扫描,这是源地址不一致、时间间隔长、没有规律的扫描。乱序扫描是对连续的端口进行扫描,这是源地址一致,时间间隔短的扫描。

(2) 被动扫描式策略。被动式策略是基于主机之上,对系统中不合适的设置、脆弱的密码以及与其他安全规则相抵触的对象进行检查。被动式扫描不会对系统造成破坏,而主动式扫描对系统进行模拟攻击,可能会对系统造成破坏。

**2. 扫描方法**

1) 密码破解

可以使用工具软件 GetNTUser 来完成。该工具可以在 WinNT4 以及 Windows 2000 操作系统上使用,主要功能包括:扫描出 NT 主机上存在的用户名,自动猜测空密码和与用户名相同的密码,可以使用指定密码字典猜测密码,可以使用指定字符来穷举猜测密码。

利用该工具可以对计算机上用户进行密码破解,首先设置密码字典,设置完密码字典以后,将会用密码字典里的每一个密码对目标用户进行测试。

要设置密码字典,先选择菜单栏“工具”下的菜单项“设置”,设置密码字典为一个文

本文件进行系统破解。利用密码字典中的密码进行破解,选择菜单栏“工具”下的菜单项“字典测试”,程序将按照字典设置进行逐一匹配,进行密码破解。

2) 开放端口扫描

了解对方开放了哪些端口也是扫描的重要一步。使用工具软件 Portscan 可以了解到对方计算机都开放了哪些端口。

3) 共享目录扫描

通过工具软件 Shed 来扫描对方主机,得到对方计算机提供了哪些目录共享。

4) 利用 TCP 协议实现端口扫描

实现端口扫描的程序可以使用 TCP 协议和 UDP 协议,原理是利用 socket 连接对方的计算机的某端口,试图和该端口建立连接。如果建立成功,就说明对方开放了该端口。如果失败了,就说明对方没有开放该端口。

5) 利用 X-Scan 进行漏洞扫描案例

目前比较典型的扫描工具有 Superscan Nmap 和 X-Scan。

X-Scan 的系统要求为 Windows 9x/NT4/2000。该软件采用多线程方式对指定 IP 地址段(或单机)进行安全漏洞检测,支持插件功能,提供了图形界面和命令行两种操作方式。

扫描内容包括远程操作系统类型及版本,标准端口状态及端口 Banner 信息,SNMP 信息,CGI 漏洞,IIS 漏洞,RPC 漏洞,SSL 漏洞,SQL Server、FTP Server、SMTP Server、POP3 Server 、NT Server 弱密码用户,NT 服务器 NETBIOS 信息注册表信息等。

(1) 主界面

主界面如图 6-1 所示。

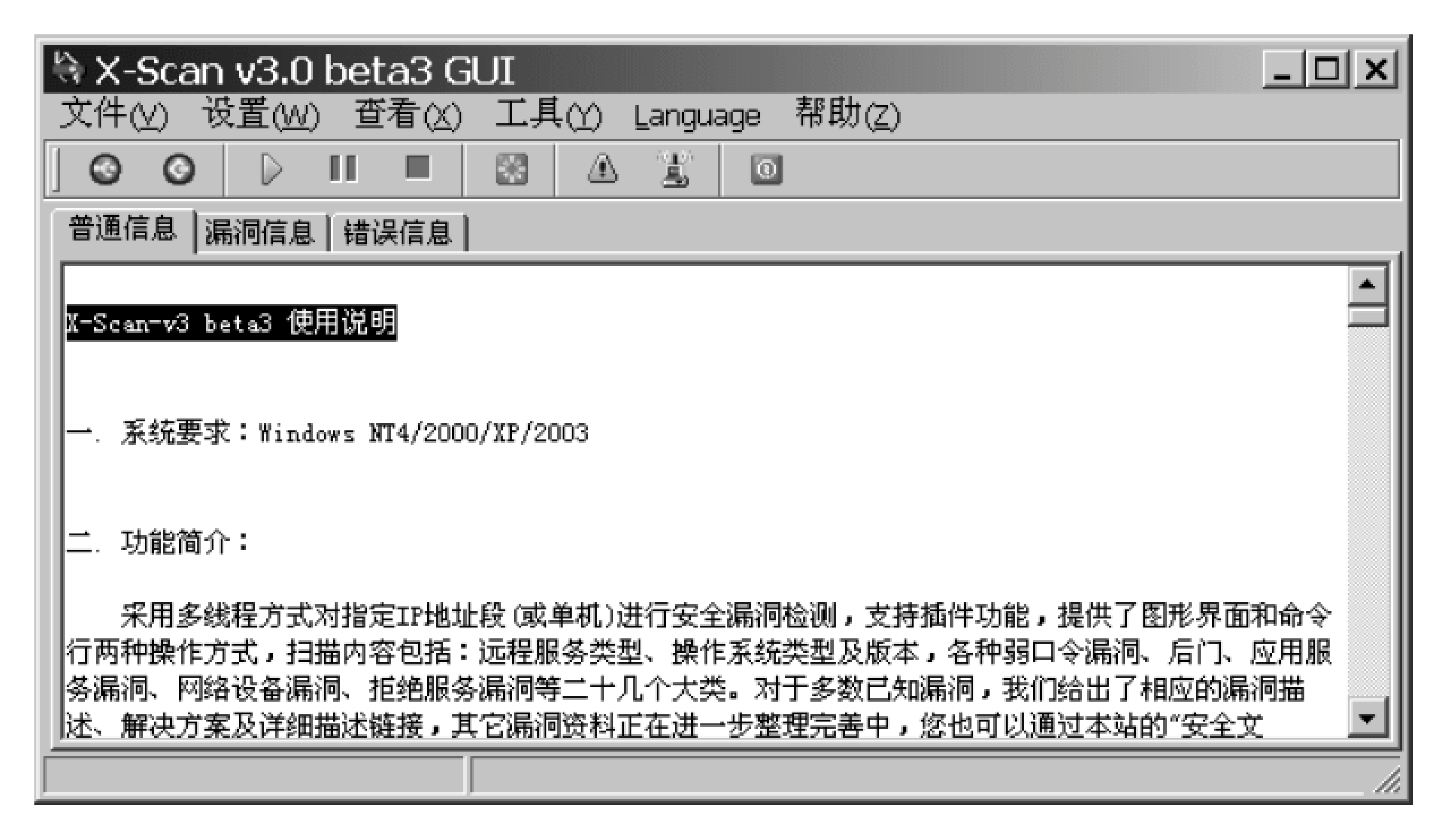



**图 6-1 X-Scan 主界面**

(2) 扫描参数

可以利用该软件对系统存在的一些漏洞进行扫描,选择设置菜单下的“扫描模块”命令,如图 6-2 所示。

可以看出该软件可以对常用的网络以及系统的漏洞进行全面的扫描,选中几个复选框,单击“确定”按钮。

下面需要确定要扫描主机的 IP 地址或者 IP 地址段,选择设置菜单下的“扫描参数”

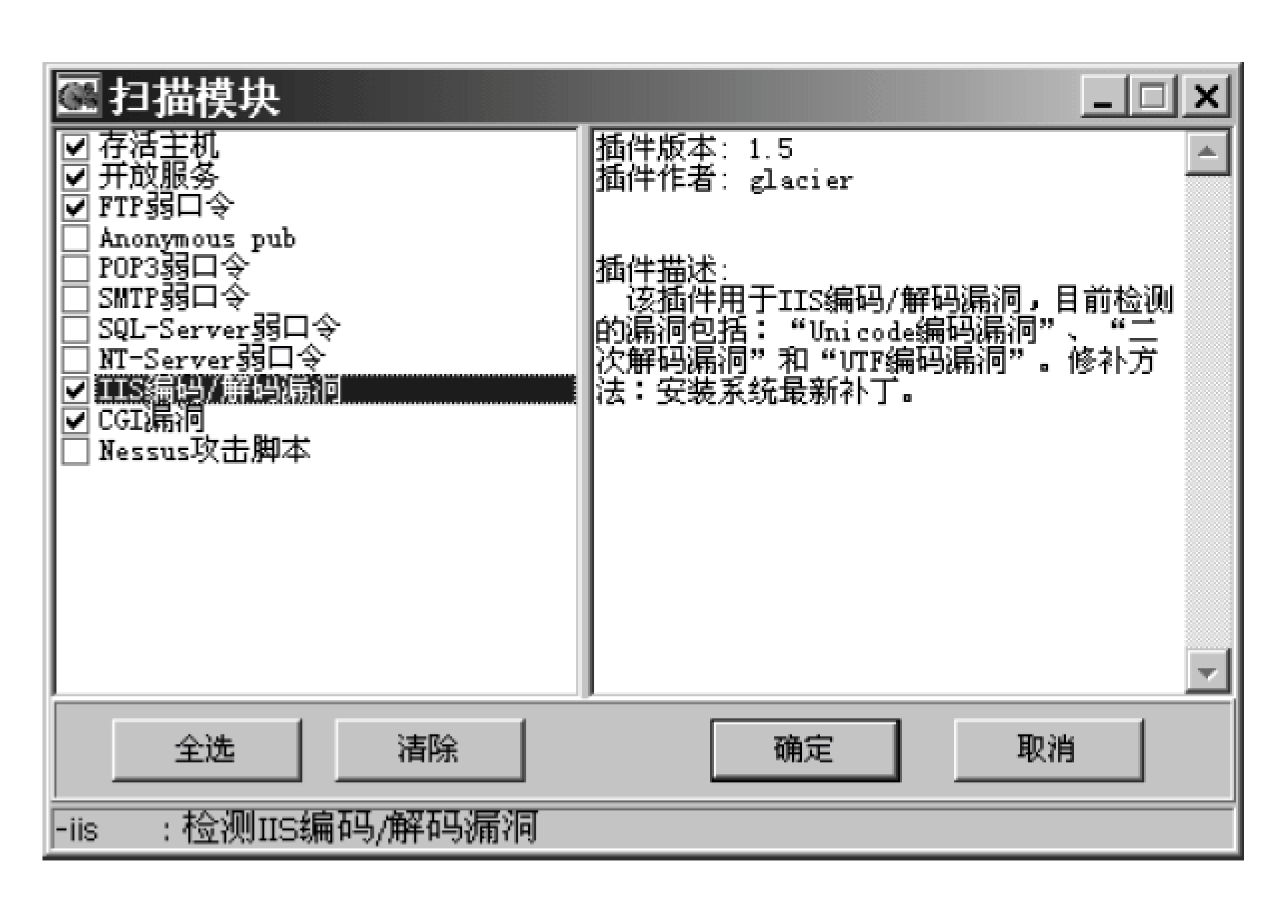



图 6-2 扫描模块设置

命令。要扫描一台主机，可以在"指定 IP 范围"框中输入"172.18.25.109-172.18.25.109"，如图 6-3 所示。

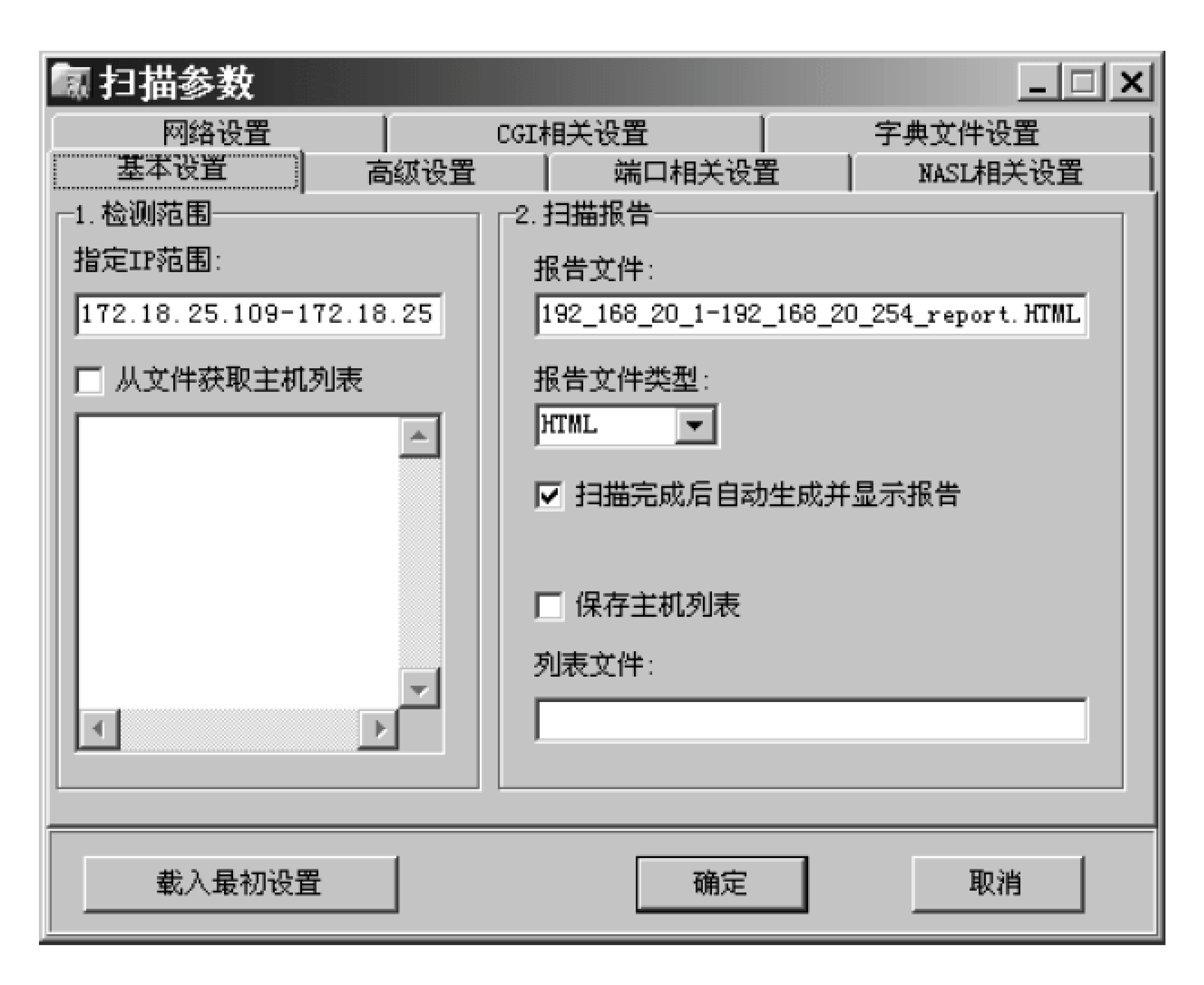



图 6-3 扫描主机 IP 地址设置

(3) 漏洞扫描

设置完毕后，进行漏洞扫描，单击工具栏上的"开始"图标，开始对目标主机进行扫描，如图 6-4 所示。

### 3. 漏洞入侵

由于宽带越来越普及，给自己的 Windows 2000 或是 XP 装上简单易学的 IIS，搭建一个不定时开放的 FTP 或者 Web 站点，相信是不少电脑爱好者所向往的，而且应该也有很多人这样做了。但是 IIS 层出不穷的漏洞实在令人担心，远程攻击者只要使用 Webdavx3 这个漏洞攻击程序和 telnet 命令就可以完成一次对 IIS 的远程攻击。

利用 IIS 的 Webdav 漏洞攻击成功后，黑客此刻执行的任何命令都是在被入侵的机器上运行的。这个时候如果执行 format 命令，危害就可想而知了，用 net user 命令添加

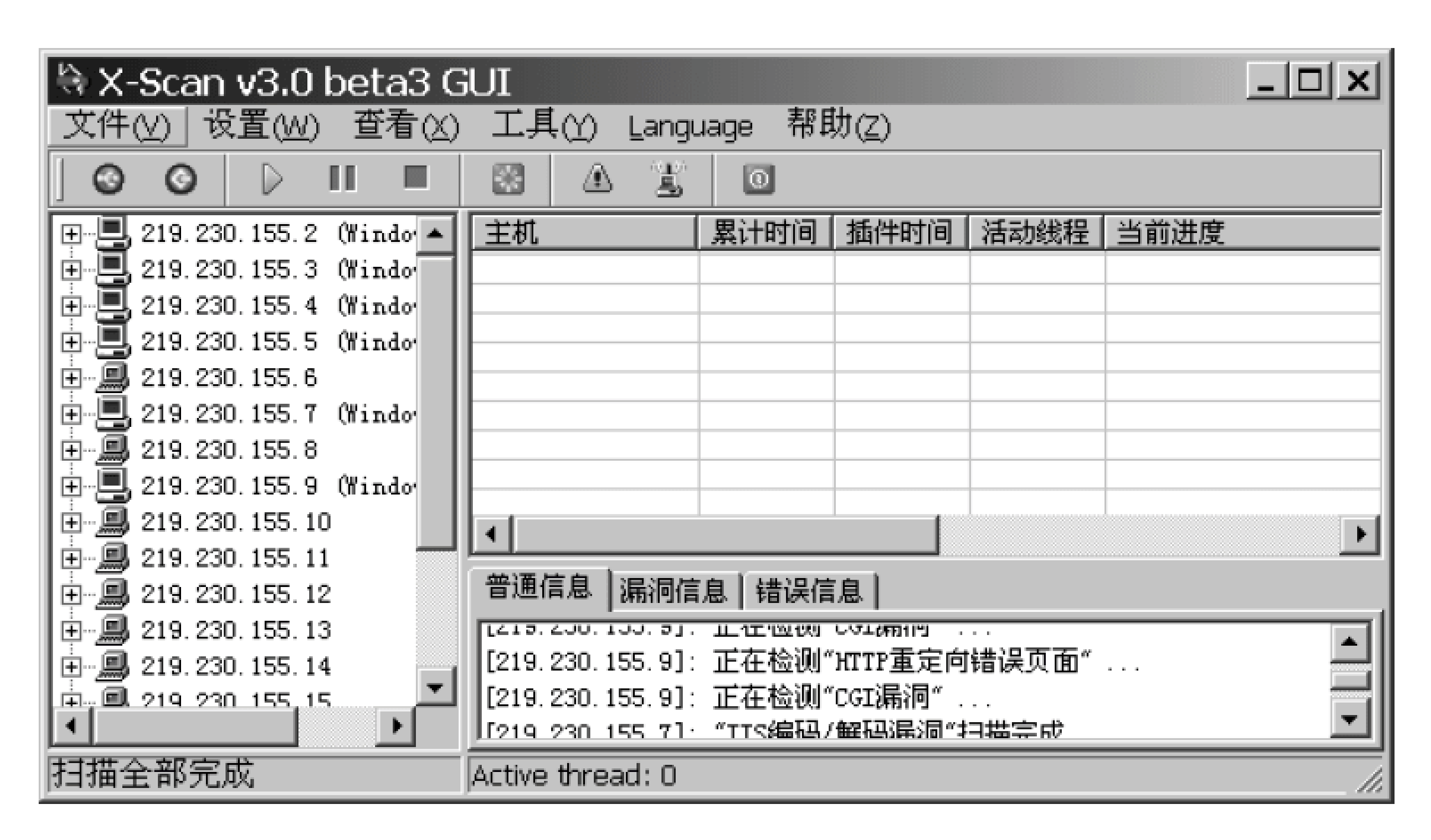



图 6-4 扫描结果

账户也是轻而易举的。

#### 4. 端口攻击

通过扫描得知被攻击计算机的漏洞后，就可很容易控制其攻击对象了。比如，一般 Windows 2000 服务器基本都有远程管理服务，并开启了 3389 端口，利用这个端口可以直接在远程控制计算机。如果在被控制的服务器中再安装 Radmin 远程控制软件，那么此软件再启动后会监听 4899 端口，这样通过客户端连接上服务器通过密码认证后就可以控制远程服务器进行一些文件操作等危害性攻击。

### 6.2.3 网络监听

网络监听工具是提供给管理员的一类管理工具。使用这种工具，可以监视网络的状态、数据流动情况以及网络传输的信息。但是网络监听工具也是黑客们常用的工具。当信息以明文的形式在网络上传输时，可以使用网络监听的方式来进行攻击。将网络接口设置在监听模式，便可以源源不断地将网上传输的信息截获。网络监听可以在网上的任何一个位置实施，如局域网中的一台主机、网关上或远程网的调制解调器之间等。网络监听最有用的是获得用户密码，当密码被截获时，就可以非常容易地登录另一台主机。

#### 1. 网络监听概述

网络监听的目的是截获通信的内容，监听的手段是对协议进行分析。Sniffer Pro 就是一个完善的网络监听工具。

监听器 Sniffer 的原理：在局域网中与其他计算机进行数据交换的时候，发送的数据包是广播出去的，在报头中包含目标机的正确地址。因此，只有与数据包中目标地址一致的那台主机才会接收数据包，其他的机器都会将包丢弃。但是，当主机工作在监听模式下时，无论接收到的数据包中目标地址是什么，主机都将其接收下来。然后对数据包进行分析，就得到了局域网中通信的数据。一台计算机可以监听同一网段所有的数据

包，不能监听不同网段的计算机传输的信息。

监听软件除 Sniffer Pro（后面将有详细的介绍）以外，还有一些常用的监听软件，如嗅探经典 Iris、密码监听工具 Win Sniffer、密码监听工具 Pswmonitor 和非变换环境局域网的 fssniffer 等。

**2. 网络监听案例**

1）利用 Win Sniffer 监听密码

Win Sniffer 专门用来截取局域网内的密码，比如登录 FTP、登录 E-mail 等的密码。

（1）设置

只要做简单的设置就可以进行密码抓取了，单击工具栏 Adapter 图标，设置网卡，这里设置为本机的物理网卡就可以。

（2）抓取密码

打开 Win Sniffer，可以看到的网络中的通信会话过程已经被记录下来，并且显示了会话的一些基本信息，从中可以抓取到相关网络应用的用户名和密码。

2）利用 Pswmonitor 监听信箱密码

监听器 Pswmonitor 用于监听基于 Web 的邮箱密码、POP3 收信密码和 FTP 登录密码等。只需在一台计算机上运行，就可以监听局域网内任意一台计算机登录的用户名和密码，并将密码显示、保存，或发送到用户指定的邮箱。

该工具软件功能比较强大，可以监听一个网段所有的用户名和密码，而且还可以指定发送的邮箱。

## 6.2.4 密码攻击

密码攻击是最古老的网络攻击方式，它是通过使用工具获取用户的账户和密码、利用用户的弱密码或者空密码对计算机实施攻击。

**1. 获取密码实施攻击**

获取密码的方式有三种。

1）默认的登录界面攻击法

在被攻击主机上启动一个可执行程序，该程序显示一个伪造的登录界面。当用户在这个伪装的界面上键入登录信息（用户名、密码等）后，程序将用户输入的信息传送到攻击者主机，然后关闭界面给出提示信息"系统故障"，要求用户重新登录。此后，才会出现真正的登录界面。

2）通过网络监听非法得到用户密码

这类方法有一定的局限性，但危害性极大，监听者往往能够获得其所在网段的所有用户的账号和密码，对局域网安全威胁巨大。

3）利用软件强行破解用户密码

在知道用户的账号后（如电子邮件"@"前面的部分），利用一些专门软件强行破解用户密码，这种方法不受网段限制，但黑客要有足够的耐心和时间。对安全系数较高的密

码破解往往需要很长时间,但对那些密码安全系数极低的用户(如某用户账号为zhanmin,其密码就是zhanaim123、minzhan,或者1234567、88888888等)只要短短的一两分钟,甚至几十秒内就可以将其破解。

在获取用户的账户和密码后,就可以对其实施攻击了。比如利用拥有某IP的用户名和密码,做IPC$入侵。IPC$即Internet Process Connection,是共享"命名管道"的资源。它是为了让进程间通信而开放的命名管道,可以通过验证用户名和密码获得相应的权限,在与远程管理计算机的共享资源时使用。

**2. 利用弱密码的入侵**

弱密码是指没有实际效力的密码,只需简单方法就可非法获取,可利用流光4.7这个软件(该版本要打IP补丁,不然不可扫国内IP主机)。下面是利用SQL的sa账户空密码入侵实例。

在Windows 2000机器上装了MSSQL的话,机器就会打开1433端口。如果MSSQL是默认安装的话,用户名是sa,密码是空的,那么就可以用SuperSQLEXEC.exe连接上去。

用SuperSQLEXEC连接成功,如图6-5所示。

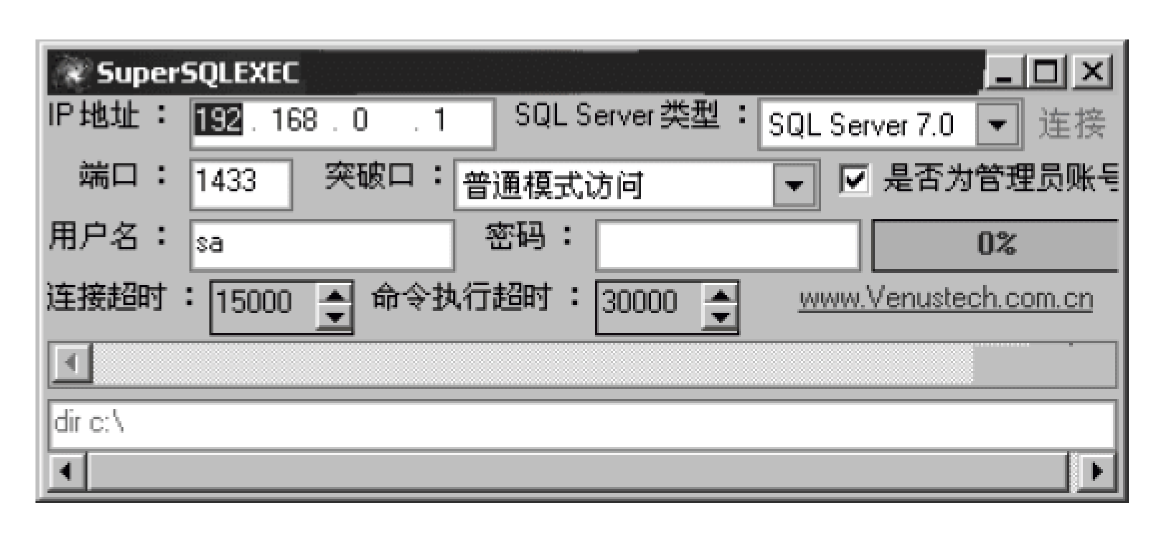



图6-5 SuperSQLEXEC界面

在命令行中输入:

```
net user guest /active:yes
The command completed successfully (>指已经被攻击的计算机回显,下同)
net user guest 123456
> The command completed successfully
net localgroup administrators guest /add
> The command completed successfully.
```

这几个命令做完后,就将guest用户激活,密码设为123456,并提升为admin。

## 6.2.5 后门攻击(特洛伊木马)

特洛伊木马是一些表面有用的软件程序,实际目的是危害计算机安全性并破坏计算机。最近的特洛伊木马都以电子邮件的形式传播,邮件的附件一般声称是Microsoft安全更新程序,但实际上是一些试图禁用防病毒软件和防火墙软件的病毒。

### 1. 特洛伊木马程序的发作表现及其发展历史

如果用户计算机中了木马，那么发作时的情况多种多样，常见表现如下。

(1) 计算机有时死机，有时又重新启动。

(2) 莫名其妙地读写硬盘或软驱、光驱莫名其妙地开仓。

(3) 用户并没有运行大的程序，系统速度变慢，系统资源占用变多。

(4) 任务管理器中出现一个陌生而奇怪的进程名，它们明显不应该出现在这里。

出现了上述现象，说明用户计算机有可能中了木马，当然也有可能是其他病毒在作怪。特洛伊木马具有隐蔽性，这是木马程序的一大特点，同时也是它与远程控制类软件(如 Windows 自带的"远程桌面连接")的主要区别。

特洛伊木马程序发展至今，已经经历了 4 代。

(1) 第一代木马，即简单的密码窃取，发送等。

(2) 第二代木马在技术上有了很大的进步。"冰河"是典型代表之一。

(3) 第三代木马在数据传输技术上做了不小的改进，出现了 ICMP 等类型的木马，利用畸形报文传递数据，增加了查杀的难度。

(4) 第四代木马在进程隐藏方面做了大的改动，采用了内核插入式的嵌入方式，利用远程插入线程技术，嵌入 DLL 线程，或者挂接 PSAPI，实现木马程序的隐藏。

### 2. 特洛伊木马类型

特洛伊木马主要分为 5 大类。

1) 远程访问型

这种程序的目的就是访问受害者的硬盘，做一些受害者可以做的事，找一些自己想要的东西。

2) 毁坏型

这种类型的程序非常危险，它可以将用户硬盘上的所有文件删除。

3) 键盘记录型

记录用户的键盘敲击，并在 Log 文件中查找密码。

4) 密码发送型

木马程序找到系统中的隐藏密码，将它发送到指定的信箱中。

5) FTP 型

木马程序打开所在计算机的 FTP 端口，使他人可以跳过密码上传或下载。

### 3. 特洛伊木马技术原理

特洛伊木马是一种基于 C/S 架构的网络通信软件，一般情况下可分为客户端程序和服务器端程序两部分，其中服务器端在目标计算机上驻留，客户端被控制者操纵。通常情况下，由客户端程序通过某种方法，主动与服务器端程序连接并建立通信关系，对目标计算机进行操纵。现在比较流行的"反弹端口"的木马，由服务器端主动向客户端发出建立连接的请求并建立通信关系。著名的木马"灰鸽子"就采用了这种技术。

特洛伊木马可以通过多种方法与特定的程序进行关联,当目标计算机系统启动后,如果用户不幸打开了被木马用来关联的程序,则木马的服务器端程序将被激活,并开始打开端口,建立与远程对应的客户端程序的通信。通过打开的端口,服务器端程序对目标计算机进行未授权的侦听。在侦听过程中,它可接收并执行来自客户端的指令,诸如删除文件、重启计算机等非法操作,并将目标计算机的一些秘密信息送往客户端。

可见,特洛伊木马对网络上的计算机的安全性和信息的秘密性构成了极大的威胁。计算机一旦被植入木马,攻击者便可进行远程控制,目标计算机将毫无安全和秘密可言。

#### 4. 特洛伊木马的植入技术

特洛伊木马植入技术,是指利用各种途径把木马的服务器端植入目标机器的方法。传统木马的植入主要靠伪装欺骗,也就是更改木马服务器端程序文件的后缀名和图标,将其伪装成一个有用的程序、文本文件或多媒体文件等,然后通过以下几种方式植入。

(1) 利用电子邮件的附件,并在受骗用户点击相应藏有木马程序的文件图标时自动完成木马的植入。

(2) 通过即时通信软件,如 QQ、MSN 等,向目标机器传送文件,并在受骗用户接收藏有木马程序的文件时自动完成木马的植入。

(3) 在网站上提供软件下载的链接供用户下载软件,其实用户下载的是伪装的木马程序。一旦用户下载并完成安装,则木马就悄然植入。

(4) 做成 BT 种子文件,在用户用 BT 软件下载文件时植入。

木马除了具有远程控制工具的功能外,通常还具有隐蔽性、秘密性、破坏性等特点。木马就如同你肩膀后的一双眼睛,它盯着你输入账号密码。在用户访问真实的银行网站之前它一直处于休眠状态,而用户访问相关网站时便会激活它,并对登录过程进行秘密监控。

利用木马达到控制主机目的的入侵造成的损失最为严重。而黑客就是通过种植服务器木马达到长期控制主机的入侵目的。所以说,如何防黑客入侵其实就是如何预防黑客种植木马和如何查杀木马。

### 6.2.6 拒绝服务攻击

拒绝服务攻击是指一个用户占据了大量的共享资源,使系统没有剩余的资源给其他用户可用的攻击。它主要用来攻击域名服务器、路由器以及其他网络服务,使被攻击者无法提供对网络的服务。

#### 1. 攻击方式

1) 服务过载

当大量的服务请求发向一台计算机中的服务进程时,就会发生服务过载。在分时机制中,这些潮水般的请求使得计算机十分忙碌地处理这些不断到来的服务请求,以至于无法处理常规的任务。同时,许多新到来的请求被丢弃,因为没有空间来存放这些请求。如果攻击的是同一个基于 TCP 协议的服务,那么这些请求的包还会被重发,结果更加重

了网络的负担。这种攻击方式会阻止系统提供特定的服务。

2）消息流

消息流发生于用户向一台网络上的目标主机发送大量的数据包，来延缓目标主机的处理速度，阻止它处理正常的任务这种情况。这些请求可能是请求文件服务、要求登录或者仅仅是简单的要求响应包（如 ping）。无论是什么形式，这些潮水般的服务请求，加重了目标主机的处理器负载，使目标主机消耗了大量的资源来响应这些请求。这种攻击可以引起目标主机因为没有内存来做缓冲以存放到来的请求，或者因为其他错误而死机。这种拒绝服务的攻击主要针对网络服务器。

3）信号接地

这种方法是一种物理方法，将网络的电缆接地、引入一些其他信号或者将以太网上的端接器拿走，都可以有效地阻止客户发送或者接收消息。这种攻击方式不仅可以阻止那些依赖服务器提供程序和资源的各种机器，也可以阻止向主服务器汇报错误的登录请求或者危险的行动，来掩盖一次非法访问的企图。

4）DDoS 攻击

DDoS 由 DoS 攻击演变而来，这种攻击是黑客利用在已经侵入并已被控制（可能是数百，甚至成千上万台）的机器上安装 DoS 服务程序，这些被控制机器即是所谓的"傀儡计算机"（zombie）。它们等待来自中央攻击控制中心的命令。中央攻击控制中心在适时启动全体受控主机的 DoS 服务进程，让它们对一个特定目标发送尽可能多的网络访问请求，形成一股 DoS 洪流冲击目标系统，猛烈的 DoS 攻击同一个网站。DDoS 攻击原理如图 6-6 所示。目前，攻击者最常用的 DDoS 攻击工具有四种：Trinoo、TFN、TFN2 和 Stacheldraht。

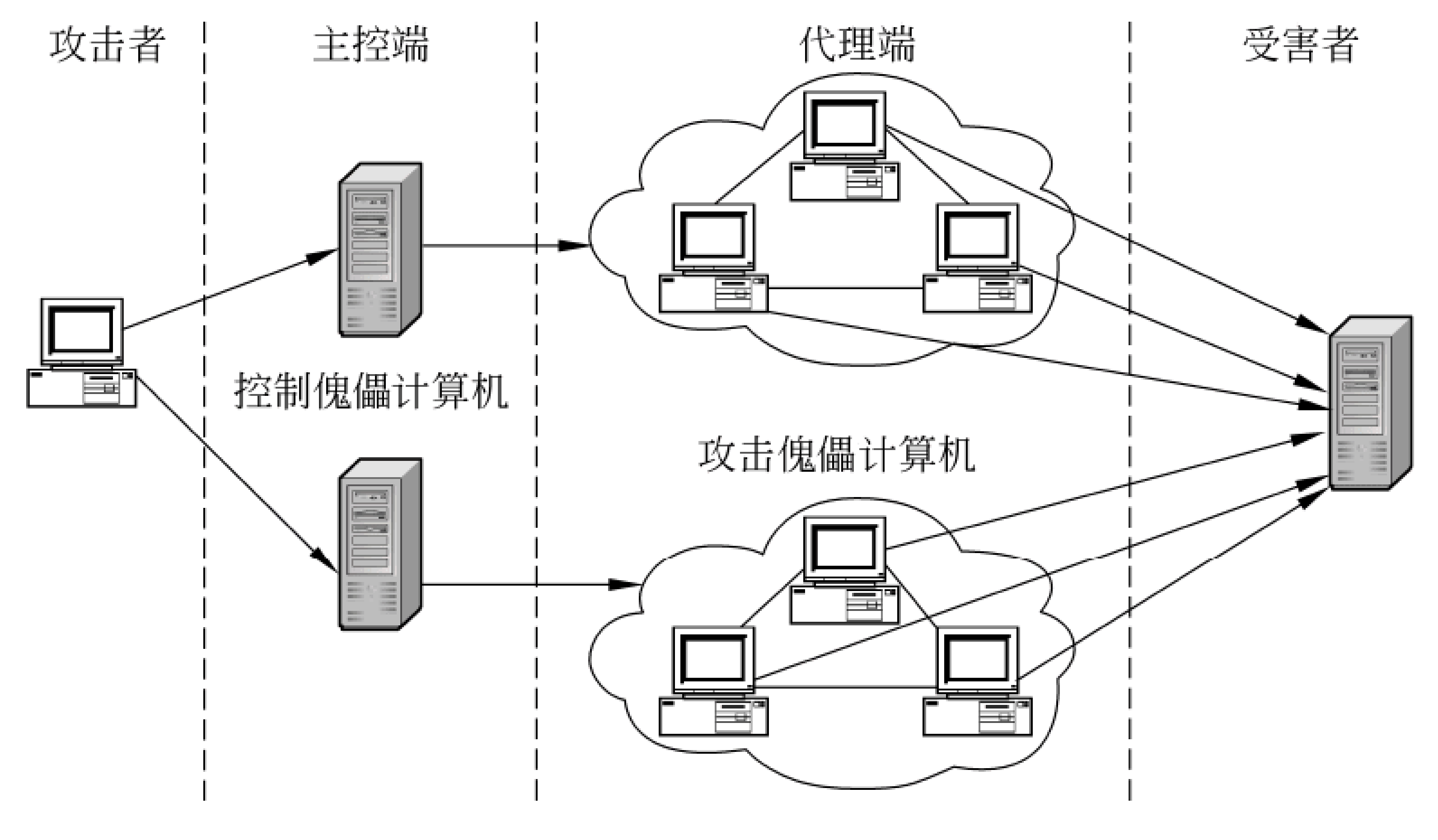



**图 6-6　DDoS 攻击原理图**

## 2. 攻击方法

1）Land 攻击

攻击特征：用于 Land 攻击的数据包中的源地址和目标地址是相同的，因为当操作

系统接收到这类数据包时，不知道该如何处理堆栈中通信源地址和目的地址相同的这种情况，或者循环发送和接收该数据包。消耗大量的系统资源，从而有可能造成系统崩溃或死机等现象。

检测方法：判断网络数据包的源地址和目标地址是否相同。

反攻击方法：适当配置防火墙设备或过滤路由器的过滤规则就可以防止这种攻击行为，并对这种攻击进行记录（记录事件发生的时间以及源主机和目标主机的 MAC 地址和 IP 地址）。

2）Package Flood 攻击

攻击特征：它是利用 TCP 客户机与服务器之间三向沟通过程的缺陷来进行的。常见的 Package Flood 有 3 种：SYN Flood、ICMP Flood、UDP Flood。这三种技术的实现方法是类似的，攻击者通过伪造源 IP 地址向被攻击者发送大量的请求，当被攻击主机接收到大量的请求时，需要使用大量的缓存来处理这些连接，并将这些请求发送回错误的 IP 地址，并一直等待回应，最终导致缓存用完，不能再处理其他合法的请求连接，导致不能对外提供正常服务。

如图 6-7 所示，攻击者的 IP 地址为 221.19.30.4，目标主机的 IP 地址为 202.190.12.3。首先攻击者将其 IP 地址伪装成 202.11.3.4，然后不断向目标主机发送 ICMP echo 请求。目标主机在收到请求后建立缓存以保存这次会话，并向请求地址 202.11.3.4 发送 SYS/ACK 响应，等待主机 202.11.3.4 的下一个确认。实际上，这种确认是等不到的。这就会造成 202.190.12.3 这台主机消耗大量的内存，最终导致其不再有能力接收其他服务请求甚至崩溃。

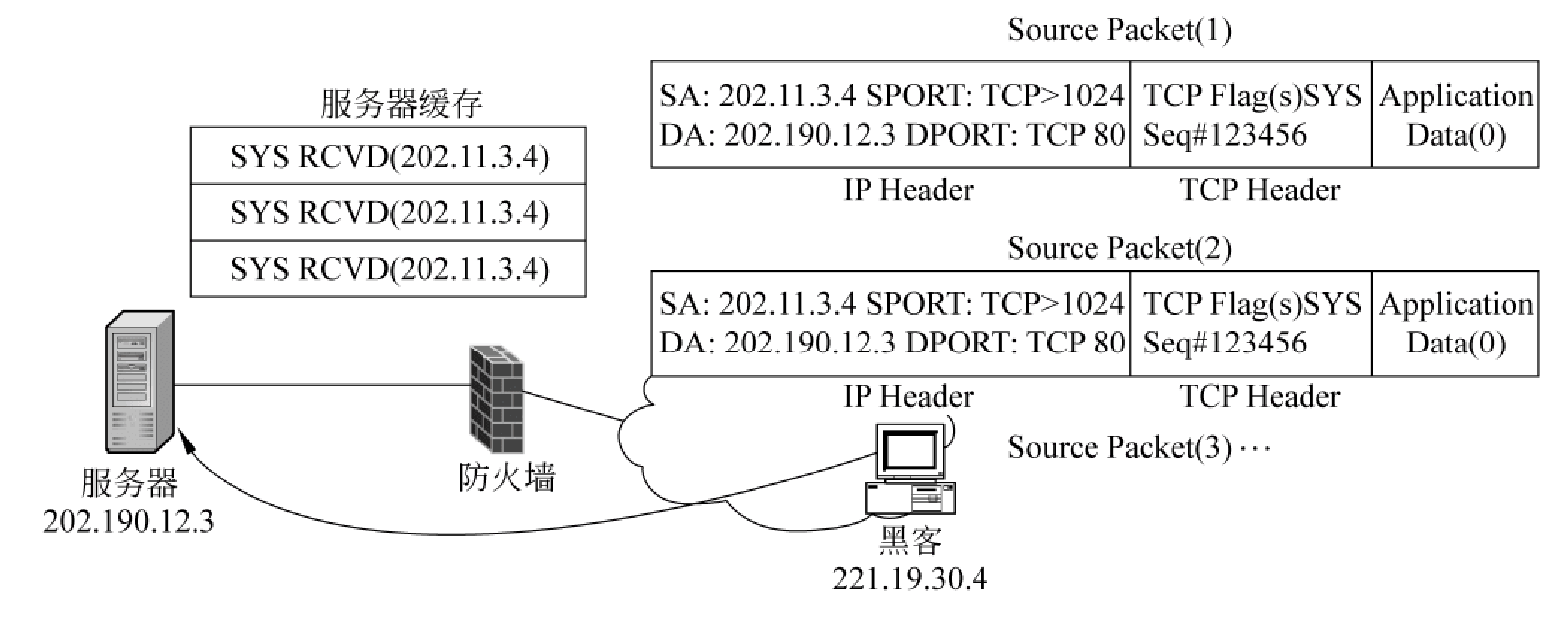



**图 6-7　SYS Plood 攻击原理**

检测方法：检查单位时间内收到的 SYN 连接是否超过系统设定的值。

反攻击方法：当接收到大量的 SYN 数据包时，通知防火墙阻断连接请求或丢弃这些数据包，并进行系统审计。

3）ping of Death 攻击

攻击特征：该攻击数据包大于 65 535 个字节。由于部分操作系统接收到长度大于 65 535 个字节的数据包时，就会造成内存溢出、系统崩溃、重启、内核失败等后果，从而达

到攻击的目的。

检测方法：判断数据包的大小是否大于 65 535 个字节。

反攻击方法：使用新的补丁程序，当收到大于 65 535 个字节的数据包时，丢弃该数据包，并进行系统审计。

4）winNuke 攻击

攻击特征：winNuke 攻击又称带外传输攻击。它的特征是攻击目标端口，被攻击的目标端口通常是 139、138、137、113、53，而且 URG 位设为 1，即紧急模式。

检测方法：判断数据包目标端口是否为 139、138、137 等，并判断 URG 位是否为 1。

反攻击方法：适当配置防火墙设备或过滤路由器就可以防止这种攻击手段（丢弃该数据包），并对这种攻击进行审计（记录事件发生的时间以及源主机和目标主机的 MAC 地址和 IP 地址 MAC）。

5）Teardrop 攻击

攻击特征：Teardrop 是基于 UDP 的病态分片数据包的攻击方法。其工作原理是向被攻击者发送多个分片的 IP 包（IP 分片数据包中包括该分片数据包属于哪个数据包以及在数据包中的位置等信息）。某些操作系统收到含有重叠偏移的伪造分片数据包时将会出现系统崩溃、重启等现象。

检测方法：对接收到的分片数据包进行分析，计算数据包的片偏移量（Offset）是否有误。

反攻击方法：添加系统补丁程序，丢弃收到的病态分片数据包并对这种攻击进行审计。

6）Smurf 攻击

Smurf 攻击是以最初发动这种攻击的程序名 Smurf 来命名。这种攻击方法结合使用了 IP 欺骗和 ICMP 回复方法，使大量网络传输充斥目标系统，引起目标系统拒绝为正常系统进行服务。

攻击特征：攻击者向一个具有大量主机和 Internet 连接的网络的广播地址发送一个欺骗性 ping 分组（echo 请求），这个目标网络被称为反弹站点，而欺骗性 ping 分组的源地址就是攻击者希望攻击的系统。

这种攻击的前提是，假设目标网络的地址是 216.131.83.2，攻击者先将其 IP 伪装成 216.131.83.2，然后向一系列中间网络的广播地址（如 211.195.83.255）发送大量的 ICMP echo 请求包，路由器接收到这个发送给 IP 广播地址的分组后，会认为这就是广播分组，并且把以太网广播地址 FF:FF:FF:FF:FF:FF 映射过来。这样路由器从 Internet 上接收到该分组，会对本地网段中的所有主机进行广播。网段中的所有主机都会向欺骗性分组的 IP 地址发送 ICMP echo 响应信息。如果这是一个很大的以太网段，可以有 500 个以上的主机对收到的 echo 请求进行回复。其攻击原理如图 6-8 所示。

由于多数系统都会尽快地处理 ICMP 传输信息，攻击者把分组的源地址设置为目标系统，因此，目标系统都很快就会被大量的 echo 信息吞没，这样轻而易举地就能够阻止该系统处理其他任何网络传输，从而引起拒绝为正常系统服务。

检测方法：有超过 5 个 icmp echo replies 在很短时间内出现。

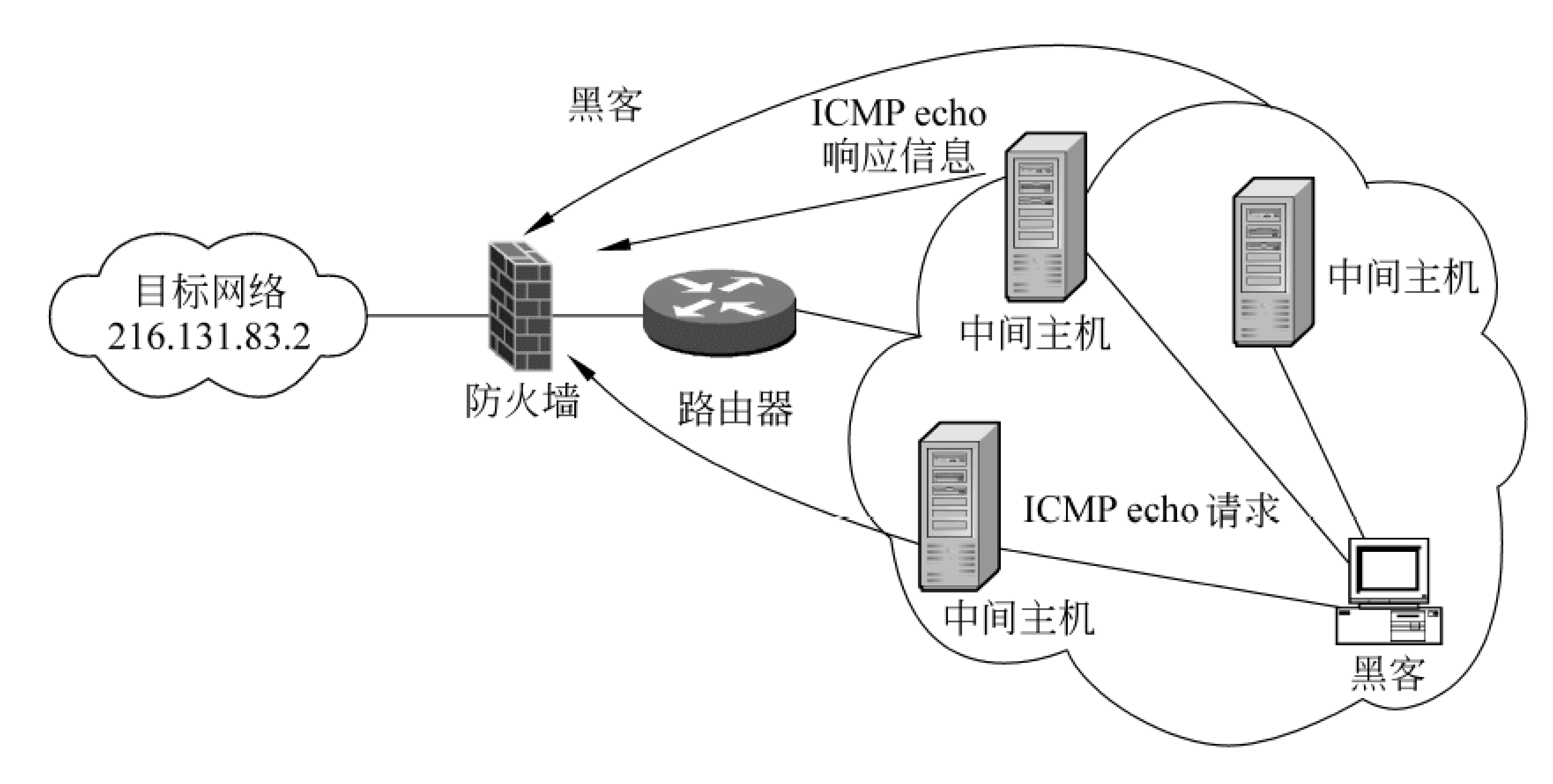



**图 6-8 Smurf 攻击原理**

反攻击方法：用户可以分别在源站点、反弹站点和目标站点三个方面采取步骤，以限制 Smurf 攻击的影响。阻塞 Smurf 攻击的源头，用户可以使用路由器的访问保证内部网络中发出的所有传输信息都具有合法的源地址。阻塞 Smurf 的反弹站点，用户使用路由器要将自己的路由器把网络广播地址映射成为 LAN 广播地址。防止 Smurf 攻击目标站点，将本网段所有路由器上的 IP 的广播功能禁止。

### 6.2.7 病毒与蠕虫攻击

伴随计算机应用不断广泛发展而诞生的计算机病毒，已经随着互联网的发展而成为网络安全最具威胁的要素之一。如今的病毒已经不仅仅是感染本地计算机，也可以像“蠕虫”一样通过网络传播。许多“蠕虫病毒”也像“特洛伊木马”一样，欺骗用户打开或执行恶意代码，甚至也可以在它们攻破的系统中打开“后门”或设置“远程访问”，而网络上经常出现的病毒也由一般的传统病毒感染变为蠕虫攻击，像“库尔尼科娃”蠕虫、Worm. Zush、熊猫烧香、MSN 性感相册、911 病毒、game. exe、PDSched. exe、冲击波、武汉男生病毒、蠕虫、爱虫病毒、灰背隼、小浩病毒、Worm/P2P. SpyBot. ht、愚蠢变种 F、冲击波杀手变种 F、Win32. WantJob、威金蠕虫变种 RC、Worm. DIOnlineGames. a、JAMMER2ND-JAMMER2ND. EXE、wnilogon-wnilogon. exe、费氏（Worm. Fizzer）求职信变种病毒、“口令蠕虫”病毒、“爱丽兹”病毒、SQLSlammer 病毒等。因此，目前病毒已经从单一的感染破坏本地计算机发展到病毒和黑客的复合体，具有破坏本地和攻击远程计算机系统的性质。十年来积累的令人信服的数据清楚地表明，病毒问题没有衰退的迹象，而新的垃圾邮件、网络钓鱼、恶意软件欺诈则利用很多先进的病毒技术不断自我进化。鉴于有关计算机网络安全的书籍介绍病毒方面的内容已经很多，本节将主要介绍近年来有关蠕虫攻击方面的内容。

#### 1. 网络蠕虫的定义

蠕虫本来是个生物学名词，1982 年，Xerox PARC 的 John Shoch 等人把它引入计算机领域。自 1988 年出现后到现在人们对它的认识越来越活，网络蠕虫的定义也日趋完

善。目前,较能全面反映网络蠕虫本质的定义之一是由我国郑辉提出的版本:“网络蠕虫是无须计算机使用者干预即可运行的独立程序,它通过不停地获得网络中存在漏洞的计算机上的部分或全部控制权来进行传播”。这个定义突出了网络蠕虫的主动性,即网络蠕虫的传播与计算机使用者无关,计算机系统存在漏洞是网络蠕虫实现攻击目标的前提。

蠕虫有主机蠕虫与网络蠕虫两种类型。主机蠕虫完全包含在它们运行的计算机中,并且使用网络的连接仅将自身复制到其他的计算机中,主机蠕虫在将其自身的复制加入到另外的主机后,就会终止它自身(因此,在任意给定的时刻,只有一个蠕虫的复制运行),这种蠕虫有时也叫“野兔”。网络蠕虫(worm)主要是利用操作系统和应用程序漏洞传播,通过网络的通信功能将自身从一个结点发送到另一个结点并启动运行的程序,可以造成网络服务遭到拒绝并发生死锁。

蠕虫由一个主程序和一个引导程序两部分组成。主程序一旦在机器上建立就会去收集与当前机器联网的其他机器的信息。它能通过读取公共配置文件并运行显示当前网上联机状态信息的系统实用程序来做到这一点。随后,它尝试利用前面所描述的那些缺陷去在这些远程机器上建立其引导程序。蠕虫一般是通过 1434 端口漏洞传播。

**2. 网络蠕虫与病毒的区别**

凡是能引起计算机故障,破坏计算机数据的程序统称为计算机病毒。网络蠕虫也符合计算机病毒的定义,从这个意义上说,网络蠕虫也是一种广义的计算机病毒。但网络蠕虫与计算机病毒又有许多不同之处,为了区分网络蠕虫和病毒,Spafford 重新定义了计算机病毒:“计算机病毒是一段代码,能把自身加到其他程序包括操作系统上;它不能独立运行,需要由它的宿主程序运行来激活它。”

由定义可知,病毒是附着于程序或文件中的一段计算机代码,它可在计算机与计算机之间传播,并在传播途中感染计算机。病毒可破坏软件、硬件和文件。病毒代码的明确目的是自我复制。病毒尝试将自身附加至主程序用来在计算机之间进行传播。与蠕虫病毒相比,它能够破坏硬件、软件和信息,但是如果没有人为干预,病毒是不会独自传播的(如共享文件或发送电子邮件)。

与病毒类似,蠕虫也在计算机与计算机之间自我复制,但蠕虫病毒可以自动完成复制过程,因为它接管了计算机中传输文件或信息的功能。一旦计算机感染蠕虫病毒,蠕虫即可独自传播。但最危险的是,蠕虫可大量复制。例如,蠕虫可向电子邮件地址簿中的所有联系人发送自己的副本,联系人的计算机也将执行同样的操作,结果造成多米诺效应(网络通信负担加重),业务网络和整个 Internet 的速度都将减慢。一旦新的蠕虫被释放,传播速度将非常迅速。不仅使网络堵塞,而且要花费两倍于以往的时间才能看到 Internet 网页。

通常,蠕虫传播无须人为干预,即蠕虫的传播不必通过“主机”程序或文件,并可通过网络自我复制(可能有改动)。与病毒相比,蠕虫可以消耗内存或网络带宽,并导致计算机停止响应。也可以潜入计算机系统并允许其他人远程操控计算机。例如,最近的 MyDoom 蠕虫可以打开受感染系统的“后门”,然后使用这些系统对网站发起攻击。

综上所述，网络蠕虫是利用计算机系统的漏洞主动攻击网络计算机，而一般病毒必须以其他程序文件为载体，并且只有当用户运行它依附的文件时，此病毒程序才被激活，然后感染所在文件系统。表6-2概括了网络蠕虫与计算机病毒的九项区别。

**表6-2 网络蠕虫与计算机病毒的区别**

| | 病　毒 | 蠕　虫 |
|---|---|---|
| 存在形式 | 寄生 | 独立个体 |
| 复制形式 | 插入到宿主程序（文件）中 | 自身的复制 |
| 传染机制 | 宿主程序运行 | 系统存在漏洞 |
| 攻击目标 | 针对本地文件 | 针对网络上的其他计算机 |
| 触发传染 | 计算机使用者 | 程序自身 |
| 影响重点 | 文件系统 | 网络性能、系统性能 |
| 计算机使用者角色 | 病毒传播中的关键环节 | 无关 |
| 防止措施 | 从宿主文件中摘除 | 为系统打补丁程序 |
| 对抗主体 | 计算机使用者、反病毒厂商 | 系统软件和服务软件提供商、网络管理人员 |

### 3. 网络蠕虫的传播途径

1）利用漏洞

这种方式是网络蠕虫最主要的破坏方式，利用漏洞也是网络蠕虫的一个最显著的特点。因为任何系统都免不了存在不足，运行在计算机上的系统软件和应用软件也不可避免地存在缺陷，这个缺陷就是漏洞。网络蠕虫就是利用计算机系统存在的漏洞去编写代码攻击计算机网络的。网络蠕虫攻击时，首先探测目标计算机存在的漏洞，然后根据探测到的漏洞建立传播路径，最后实施攻击。著名的振荡波蠕虫病毒利用的是计算机的LSASS漏洞，高波和冲击波蠕虫病毒都是利用的RPC Dcom缓冲溢出漏洞。

2）依赖E-mail传播

以电子邮件附件的形式进行传播是网络蠕虫采用的主要传播方式，蠕虫编写者通过向用户发送电子邮件，而用户在不知情的情况下单击了电子邮件附件时，网络蠕虫就会感染此计算机。所以，不要轻易单击陌生人的电子邮件，以免感染网络蠕虫。影响范围较广的网络天空、贝革热和小邮差等蠕虫病毒都是利用电子邮件传播的。

3）依赖网络共享

网络共享是网络蠕虫传播的重要途径之一，网络蠕虫利用共享网络资源进行传播。所以，不要随意设置共享文件夹，以免被网络蠕虫利用。比如经常作怪的尼姆达蠕虫病毒就是利用网络共享进行传播的。

4）弱密码攻击

若用户的密码很容易猜测，网络蠕虫则会在攻克了用户密码后进入计算机并获得控制权。所以，应该设置复杂的密码，增加破解难度。

## 6.2.8 缓存溢出攻击

在 1.2.4 节中已经介绍了有关缓存溢出的原理、概念及攻击方式，这里就不再赘述。下面具体介绍缓存溢出攻击的实例。

### 1. SQL 缓存溢出攻击实例

在 Windows 2000 机器上装了 mssql，机器就会打开 1433 端口。溢出 1433 需要两个工具：nc.exe 和 sql2.exe（在 www.sandflee.net 有下载）。

（1）打开一个命令提示符窗口。把下载的 nc.exe 和 sql2.exe 放在 c 盘根目录下，然后输入“c:\nc>nc-l-p 56”命令回车，如图 6-9 所示。用 nc 这个工具开一个 56 的端口监听。

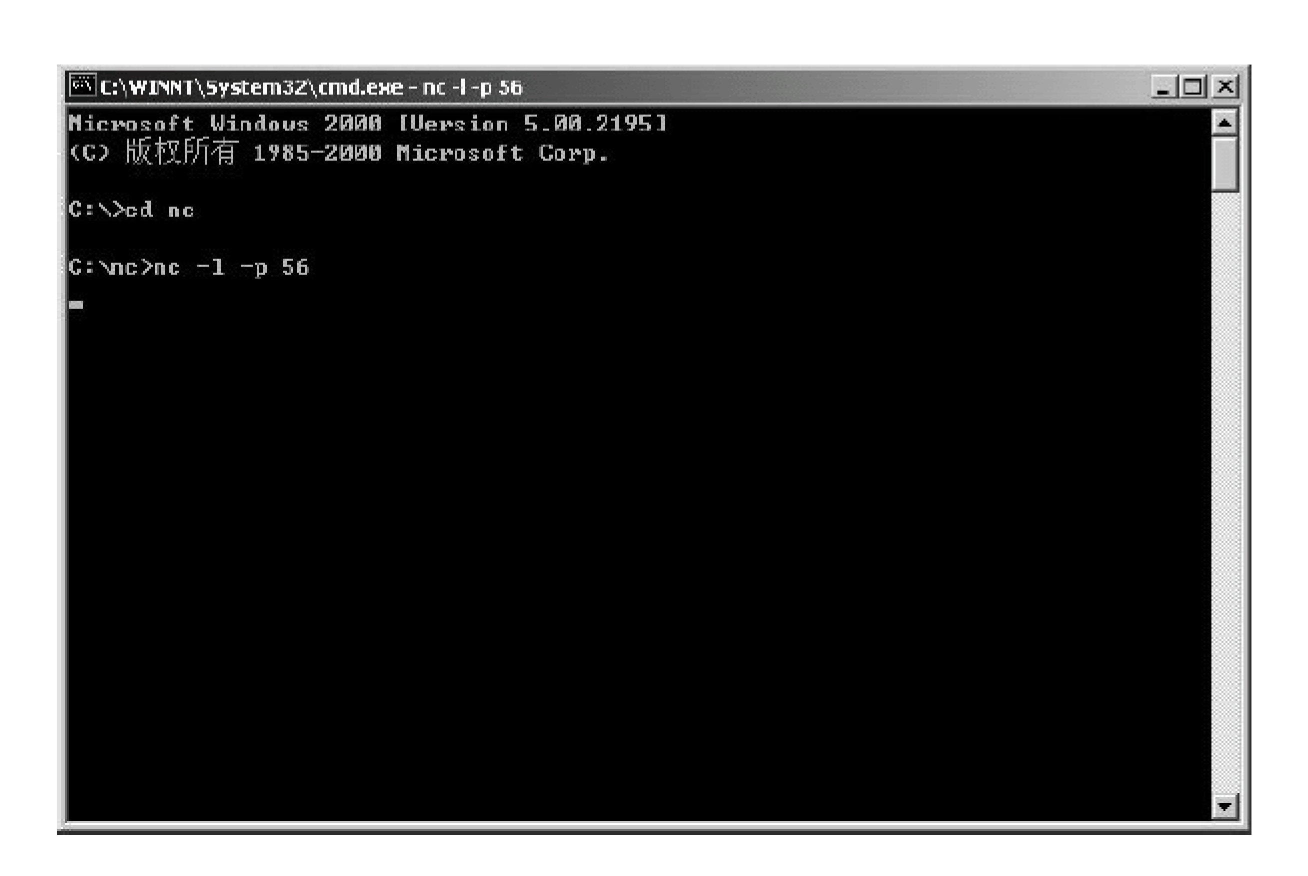



图 6-9 nc 运行窗口

（2）再打开一个命令提示符窗口。在这个窗口输入“c:\nc>sql2.exe”命令加上要入侵网站的 IP 和自己的 IP 再加上“56 0”后回车，如图 6-10 所示。

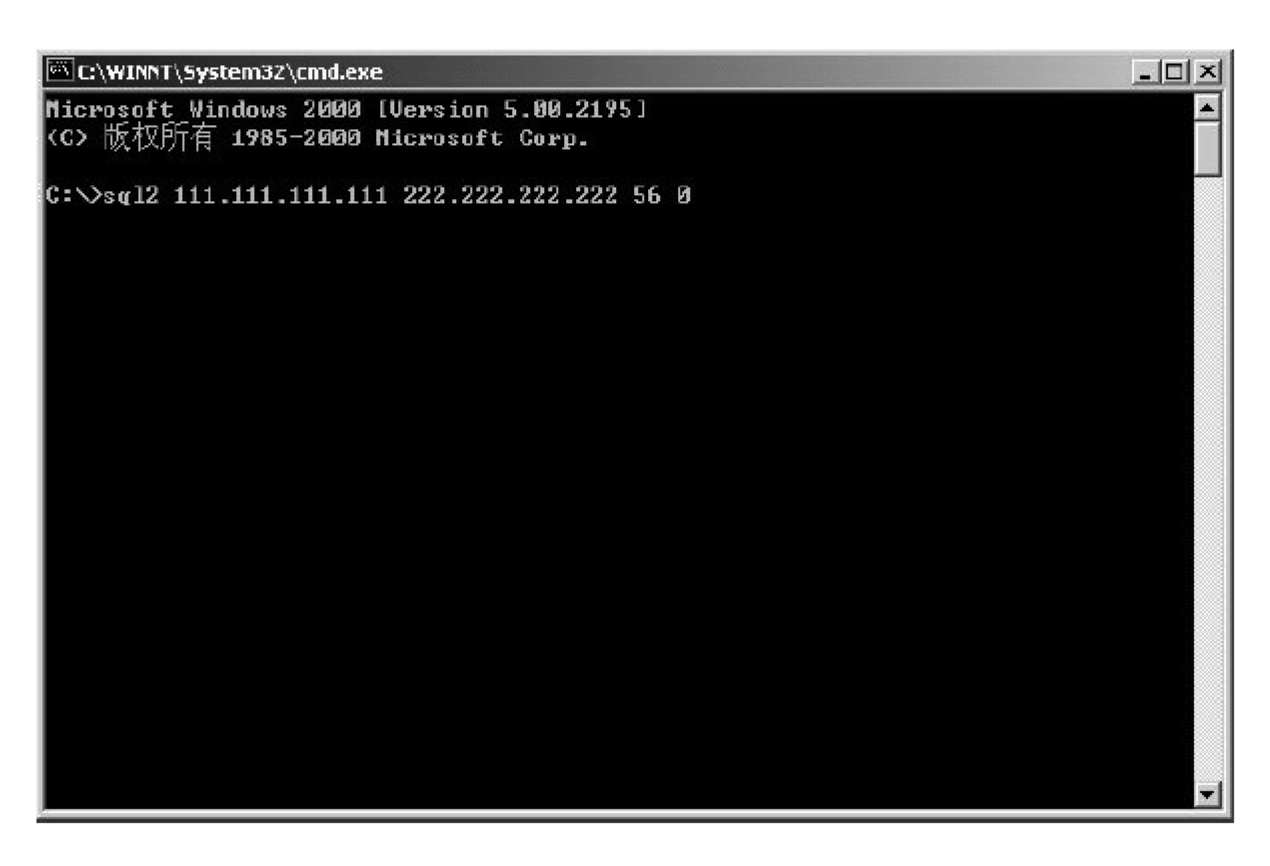



图 6-10 sql2 运行窗口

其中命令行中的 56 可以随意改成别的，好像 40 和 53 成功率高一点。如果命令中的 0 不行的话，可以试试 1 或 2。如果入侵网站存在这个漏洞的话，那么打开的第一个窗口

就会定位在被攻击者的 c:\winnt\system32F,就是说已经进入被攻击者的机器里了,如图 6-11 所示。进去以后,可以填加一个用户,使用“net user guest /active:yes 命令,将默认禁止的 guest 用户激活。再输入“net user guest 123456”命令,把 guest 的密码变成 123456,然后输入“net localgroup administrators guest /add”命令,让 guest 成为最高权限的管理员。




**图 6-11　进入被攻击系统**

以上几种入侵破坏方法,防火墙均无报警,但造成的破坏却是严重的。这对于那些自以为装上防火墙就万事大吉的人来说是沉重的打击。

### 6.2.9　其他相关攻击方式

其实黑客的攻击手段繁多,不可能一一例举,下面对在工作中经常遇到的其他类型的黑客攻击手段加以说明。

**1. 电子邮件攻击**

电子邮件系统面临着巨大的安全风险,很容易成为某些专门面向邮件攻击的目标,这些攻击有如下几种。

1) 窃取、篡改数据

通过监听数据包或者截取正在传输的信息,黑客能够读取甚至修改数据。

2) 伪造邮件

黑客伪造邮件,使它们看起来似乎发自某人、某地。

3) 拒绝服务

黑客可以让系统或者网络充斥邮件信息而瘫痪,这些邮件信息塞满队列,占用宝贵的 CPU 资源和网络带宽。黑客使用电子邮件攻击时,一般是采用电子邮件炸弹(E-mail Bomb)的方式,指用伪造的 IP 地址和电子邮件地址向同一信箱发送数以千计、万计甚至无穷多次的内容相同的恶意邮件,也可称为大容量的垃圾邮件。由于每个人的邮件信箱是有限的,当庞大的邮件垃圾到达信箱的时候,就会挤满信箱,把正常的邮件给冲掉。同时,因为它占用了大量的网络资源,常常导致网络塞车,使用户不能正常地工作,严重者

可能会给电子邮件服务器带来危险甚至瘫痪。“电子邮件炸弹”是最早的拒绝服务攻击方式之一,是一种破坏性很强的攻击。

4) 病毒

现在电子邮件使得传送文件附件更加容易,如果用户毫不设防地去执行文件附件,病毒就会感染他们的系统。

### 2. Web 欺骗

这是一种在 Internet 上使用的针对 WWW 的攻击技术,这种攻击方法会泄露某人的隐私或破坏数据的完整性,危及使用 Web 浏览器的用户。Web 站点的广泛使用,诱惑着网上的欺诈行为。这种欺诈行为是由于铺天盖地的信息,而又无法让人们辨认其真假。类似于张贴在街头的小广告,仅凭看到的一些信息,是无法分辨哪些是真,哪些是假。而 Web 上这种欺诈就更加容易了。

黑客攻击时,先编写一些看起来“合法”的程序,上传到一些 FTP 站点或是提供给某些个人主页,诱导用户下载。当一个用户下载软件时,黑客的软件一起下载到用户的机器上。该软件会跟踪用户的计算机操作,它静静地记录着用户输入的每个密码,然后把它们发送给黑客指定的 Internet 信箱。例如,有人发电子邮件给用户,声称为“确定我们的用户需要”而进行调查。作为对填写表格的回报,允许用户免费使用多少小时。但是,该程序实际上却是搜集用户的密码,并把它们发送给某个远方的“黑客”。

### 3. 利用处理程序错误的攻击

这是利用 TCP/IP 协议的处理程序中的错误进行的攻击。攻击时,黑客故意错误地设定数据包头的一些重要字段,例如,IP 包头部的 TotalLength、Fragment offset、IHL 和 source address 等字段,使用 Raw Socket 将这些错误的 IP 数据包发送出去。在接受数据端,接收程序通常都存在一些问题,因而在将接受到的数据包组装成一个完整的数据包的过程中,就使系统死机、挂起或系统崩溃。

### 4. IP 欺骗

IP 电子欺骗,就是通过伪造源于一个可信任 IP 地址的数据包使一台机器认证另一台机器的复杂技术,其实质就是让一台机器来扮演另一台机器,借以蒙混过关。其中,信任是那些获得相互连接的机器之间的一种关系。认证是这些机器用于彼此识别的过程。源地址认证带有非自身弱点,就使电子欺骗成为可能。伪造 IP 地址的目的:一方面,防止攻击者的 IP 地址被服务器记载而暴露身份;另一方面,伪造的 IP 地址可以欺骗路由器或网关中设置的防火墙,以达到攻击的目的。

一般来讲,欺骗是一种减少网络开销的技术,尤其在广域网(WAN)中。通过欺骗,让网络和路由器等设备响应远程设备的请求,从而减少必需的带宽。这项技术欺骗使 LAN 设备,即使远程 LAN 已脱离,也误认为仍旧与之相连。

欺骗的形式多种多样,从随机扫描到利用系统已知的一些漏洞。电子欺骗攻击通常发生于一台主机被确信在安全性方面存在漏洞之后。此时入侵者已做好了实施一次 IP

电子欺骗的准备，攻击者知道目标网络存在漏洞并且知道该具体攻击哪一台主机。如果黑客入侵成功，他可以控制整个 Web 站点，在网络管理人员不知情下，随心所欲地为所欲为。一般情况下，黑客在取得 IP 电子欺骗成功以后，往往会做如下事情。

1）获得较高授权

在入侵成功 Web 站点重新登记注册(往往以假名方式)，并给予较高授权，使得入侵者可以在下次“合法”地进入该 Web 站点。

2）设置“后门”程序

在入侵成功 Web 站点留下“后门”程序，入侵者在以后进入该 Web 站点可以避开检验认证程序的检查。

### 5. ARP 地址欺骗

2007 年上半年，在网络上频繁出现了一种 ARP 地址欺骗的木马，受到攻击的主机表现为不能正常上网，但是表面上一切正常，看不出问题。可用下面的方法检测自己的计算机是否中了 ARP 木马。

(1) 同时按 Ctrl+Alt+Del 组合键，选择“任务管理器”，选中“进程”标签，查看其中是否有一个名为 MIR0.dat 的进程。如果有，说明已经中毒。

(2) 单击“开始→运行”，输入“arp-d”回车，然后重新尝试上网，如能短暂正常访问，则说明此次断网是受木马病毒影响。

ARP 欺骗木马只需成功感染一台计算机，就可能导致整个局域网都无法上网，严重的甚至可能带来整个网络的瘫痪。

那什么是 ARP 地址欺骗呢？在实现 TCP/IP 协议的网络环境下，一个 IP 包走到哪里，要怎么走是靠路由表定义。但是，当 IP 包到达该网络后，哪台机器响应这个 IP 包却是靠该 IP 包中所包含的硬件 MAC 地址来识别。也就是说，只有机器的硬件 MAC 地址和该 IP 包中的硬件 MAC 地址相同的机器才会应答这个 IP 包。因为在网络中，每一台主机都会有发送 IP 包的时候，所以在每台主机的内存中，都有一个 IP 到硬件 MAC 的转换表。通常是动态的转换表(该 ARP 表可以手工添加静态条目)。也就是说，该对应表会被主机在一定的时间间隔后刷新。这个时间间隔就是 ARP 高速缓存的超时时间。

通常主机在发送一个 IP 包之前，它要到该转换表中寻找和 IP 包对应的硬件 MAC 地址。如果没有找到，该主机就发送一个 ARP 广播包。于是，主机刷新自己的 ARP 缓存，然后发出该 IP 包。

了解这些常识后，现在就可以谈一下在以太网络中如何实现 ARP 欺骗了，可以看看这样一个例子。

1）同一网段的 ARP 欺骗

如图 6-12 所示，有三台主机，其中每台主机的 IP 和 MAC 地址如下。

A 的 IP 地址是 192.168.0.1，硬件地址为

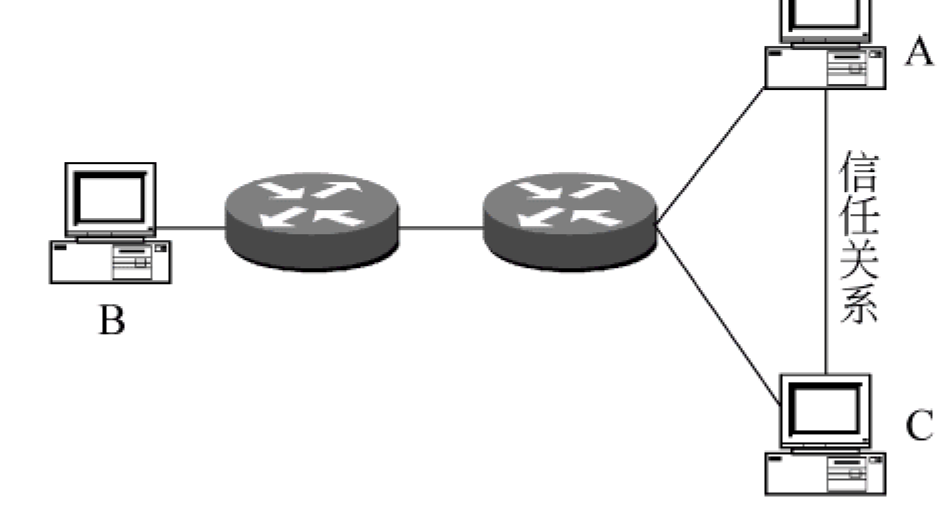


图 6-12　同一网段 ARP 欺骗

AA:AA:AA:AA:AA:AA。

B 的 IP 地址是 192.168.0.2,硬件地址为 BB:BB:BB:BB:BB:BB。

C 的 IP 地址是 192.168.0.3,硬件地址为 CC:CC:CC:CC:CC:CC。

一个位于主机 B 的入侵者想非法进入主机 A,可是这台主机上安装有防火墙。通过收集资料,他知道这台主机 A 的防火墙只对主机 C 有信任关系,开放 23 端口(telnet 端口)。而他必须要使用 Telnet 来进入主机 A,这个时候应该如何处理呢?

如果主机 A 和主机 C 之间的信任关系是建立在硬件地址 MAC 的基础上的。这个时候需要用 ARP 欺骗的手段让主机 A 把自己的 ARP 缓存中的关于 192.168.0.3 映射的硬件地址改为主机 B 的硬件地址。

可以人为地制造一个 arp_reply 的响应包,发送给想要欺骗的主机,这是可以实现的,因为协议并没有规定必须在接收到 arp_echo 后才可以发送响应包。这样的工具很多,也可以直接用 sniffer pro 抓一个 arp 响应包,然后进行修改。

可以人为地制造这个包,可以指定 ARP 包中的源 IP、目标 IP、源 MAC 地址、目标 MAC 地址。这样就可以通过虚假的 ARP 响应包来修改主机 A 上的动态 ARP 缓存达到欺骗的目的。

下面是具体的步骤。

(1) 先研究 192.0.0.3 这台主机,发现这台主机的漏洞。

(2) 根据发现的漏洞使主机 C 当掉,暂时停止工作。

(3) 这段时间里,把自己的 IP 改成 192.0.0.3。

(4) 用工具发一个源 IP 地址为 192.168.0.3,源 MAC 地址为 BB:BB:BB:BB:BB:BB 的包给主机 A,要求主机 A 更新自己的 ARP 转换表。

(5) 主机更新了 ARP 表中关于主机 C 的 IP 到 MAC 对应关系。

防火墙失效了,入侵的 IP 变成合法的 MAC 地址,可以 Telnet 了。

2) 不同网段的 ARP 欺骗

如图 6-13 所示,A、C 位于同一网段而主机 B 位于另一网段,三台机器的 IP 地址和硬件地址如下。

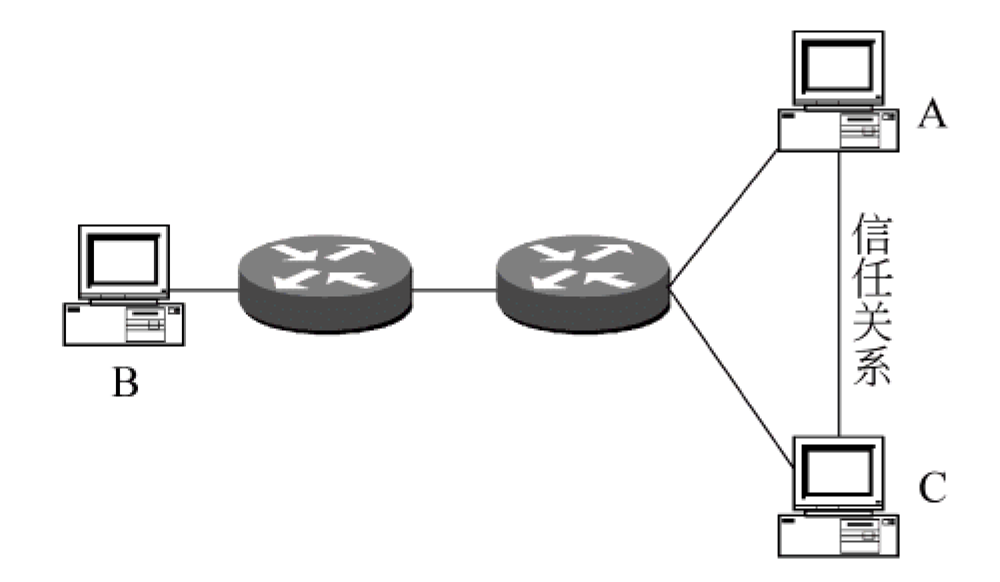


图 6-13 不同网段 ARP 欺骗

A 的 IP 地址为 192.168.0.1,硬件地址是 AA:AA:AA:AA:AA:AA。

B 的 IP 地址为 192.168.1.2,硬件地址是 BB:BB:BB:BB:BB:BB。

C 的 IP 地址为 192.168.0.3,硬件地址是 CC:CC:CC:CC:CC:CC。

在这种情况下,位于 192.168.1 网段的主机 B 如何冒充主机 C 欺骗主机 A 呢? 显然用上面的办法的话,即使欺骗成功,主机 B 和主机 A 之间也无法建立 Telnet 会话,因为路由器不会把主机 A 发给主机 B 的包向外转发,路由器会发现地址在 192.168.0 网段之内。

3) 利用 ICMP 重定向报文达到 ARP 欺骗

ICMP 重定向报文是 ICMP 控制报文中的一种。在特定的情况下,当路由器检测到

一台机器使用非优化路由的时候，它会向该主机发送一个 ICMP 重定向报文，请求主机改变路由。路由器也会把初始数据报向它的目的地转发。

可以利用 ICMP 重定向报文达到欺骗的目的。

下面是结合 ARP 欺骗和 ICMP 重定向进行攻击的步骤。

(1) 为了使自己发出的非法 IP 包能在网络上能够存活长久一点，要修改 IP 包的生存时间 TTL 为下面的过程中可能带来的问题做准备。把 TTL 改成 255(TTL 定义一个 IP 包如果在网络上到不了主机后，在网络上能存活的时间，改长一点在本例中有利于做充足的广播)。

(2) 下载一个可以自由制作各种包的工具(如 hping2)。

(3) 然后和前面一样，寻找主机 C 的漏洞，按照这个漏洞当掉主机 C。

(4) 在该网络的主机找不到原来的 192.0.0.3 后，将更新自己的 ARP 对应表。于是发送一个原 IP 地址为 192.168.0.3，硬件地址为 BB:BB:BB:BB:BB:BB 的 ARP 响应包。

(5) 构造一个 ICMP 的重定向广播。虽然现在每台主机都知道了，一个新的 MAC 地址对应 192.0.0.3，一个 ARP 欺骗完成了。但是，每台主机都只会在局域网中找这个地址，而根本就不会把发送给 192.0.0.3 的 IP 包丢给路由。

(6) 定制一个 ICMP 重定向包告诉网络中的主机：到 192.0.0.3 的路由最短路径不是局域网，而是路由。请主机重定向路由路径，把所有到 192.0.0.3 的 IP 包丢给路由。

(7) 主机 A 接受这个合理的 ICMP 重定向，于是修改自己的路由路径，把对 192.0.0.3的通信都丢给路由器。

(8) 入侵者终于可以在路由外收到来自路由内的主机 IP 包了，可以开始 Telnet 到主机的 23 端口。

其实上面的想法只是一种理想的情况，主机许可接收的 ICMP 重定向包其实有很多的限制条件，这些条件使 ICMP 重定向变得非常困难。

TCP/IP 协议实现中，关于主机接收 ICMP 重定向报文主要有下面几条限制。

(1) 新路由必须是直达的。

(2) 重定向包必须来自去往目标的当前路由。

(3) 重定向包不能通知主机用自己作路由。

(4) 被改变的路由必须是一条间接路由。

由于有这些限制，所以 ICMP 欺骗实际上很难实现。但是也可以主动地根据上面的思维寻找一些其他的方法。更为重要的是知道了这些欺骗方法的危害性，就可以采取相应的防御办法。

## 6.3 黑客攻击的主要防范措施

随着网络技术的进步，“黑客”的攻击技术在不断地变化和升级，病毒和黑客技术的结合，黑客攻击和防范黑客的对抗呈现越来越激烈的局面。单靠几个孤立的安全系统是无法防范黑客的，需要采用网络系统和个人用户安全防范相结合、多种网络安全设备相

结合的综合的防范措施。以下将论述黑客防范措施的几个方面。

## 6.3.1 使用服务器版本的操作系统

在选择网络操作系统时，要注意其提供的安全等级，尽量选用安全等级高的操作系统。美国国防部1985年提出的计算机系统评价准则，是一个计算机系统的安全性评估的标准，它使用了可信计算机TCB这一概念，即计算机硬件与支持不可信应用及不可信用户的操作系统的组合体。网络操作系统的安全等级是网络安全的根基，如果基础不好则网络安全先天不良，在此基础上很多努力将无从谈起。如有的网络采用的UNIX系统由于版本太低从而导致安全级别太低，只有C4级，而网络系统安全起码要求是C2级。1999年9月13日，由公安部提出并组织制定的强制性国家标准《计算机信息系统安全保护等级划分准则》，它通过规范、科学和公正地评定和监督管理，为计算机信息系统安全等级保护管理法则的制定和执法部门的监督检查提供依据，为计算机信息系统安全产品的研制提供技术指导。各网络管理部门应按照系统的安全等级，选用符合安全等级保护要求的网络操作系统，及时更新操作系统的版本。

在网络上提供服务的计算机一定要安装高版本的UNIX操作系统或者服务器版的操作系统(如SAS Linux或者Windows 2000 Server、Windows Server 2003)，对于个人计算机最好安装专业版的Windows 2000/XP，并随时注意操作系统厂商推出的补丁程序。

## 6.3.2 堵住系统漏洞

### 1. 安装操作系统时要注意

因为现在的硬盘越来越大，许多人在安装操作系统时希望安装越多越好。岂不知装的越多所提供的服务就越多，而系统的漏洞也就越多。如果只是要作为一个代理服务器，则只安装最小化操作系统和代理软件、杀毒软件、防火墙即可。不要安装任何应用软件，更不可安装任何上网软件用来上网下载，甚至输入法也不要安装，更不能让别人使用这台服务器。

### 2. 安装补丁程序

上面所讲的利用输入法的攻击其实就是黑客利用系统自身的漏洞进行的攻击。及时下载微软提供的补丁程序来安装，就可较好地完善系统和防御黑客利用漏洞的攻击。可下载Windows最新的Service Pack补丁程序，也可直接运行“开始”菜单中的Windows Update进行系统的自动更新。

### 3. 关闭无用的甚至有害的端口

计算机要进行网络连接就必须通过端口，而黑客要种上“木马”控制电脑也必须要通过端口。所以，可以通过关闭一些暂时无用的端口(但对于“黑客”却可能有用)，即关闭无用的服务，来减少黑客的攻击路径。可通过“控制面板”的“管理工具”来进入“服务”。

1) server服务

此服务提供 RPC 支持文件打印以及命名共享，关掉它就关掉 Windows 2000 的默认共享，比如 IPC $（可用于 net 命令攻击）、c $（C 盘共享）、ADMIN $（winnt\system32 目录共享），最好还要取消网络中的文件和打印共享。

如果要禁止 C $、D $、E $ 一类根目录的共享，可以单击"开始→运行"命令，在运行窗口键入 Regedit 后回车，打开注册表编辑器，随后依次展开[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters]分支，将右侧窗口中"AutoShareServer"的键值设置为 0 即可（如没有可新建该值）。

如果要禁止 ADMIN $ 共享，可以在同样的分支下，将右侧窗口中 AutoShareWKs 的键值设置为 0（如没有可新建该值）。如果要禁止 IPC $ 共享，可以在注册表编辑器中依次展开[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]分支，将右侧窗口中 restrictanonymous 的键值设置值为 1 即可。

如在进行上述操作后操作系统仍然出现共享根目录的现象，那需要使用杀毒软件来进一步检查系统。

2）木马及蠕虫攻端口

（1）23 端口

通过关闭 Telnet 服务即可禁止 Telnet 服务（该服务可使远程用户登录到系统并且使用命令运行控制台程序）。

（2）3389 端口

3389 端口是 Windows 的远程管理终端所开的端口，请先确定该服务是否是用户自己开放的。如果不是必需的，要关闭该服务。在管理工具-终端服务配置-连接-RDP-TCP 属性-远程控制-选"不允许远程控制"来关闭 3389 等一些无用的端口。在 Windwos 2000 中关闭的方法是打开服务管理器，找到 Terminal Services 服务项，在属性选项中将启动类型改成手动，并停止该服务。Windows XP 关闭的方法是在"我的电脑"上右击选择"属性"进入"远程"选项页，将里面的远程协助和远程桌面两个选项框里的勾去掉。

（3）4899 端口

首先说明 4899 端口是远程控制软件（remote administrator）服务端监听的端口，不能算是一个木马程序，但是具有远程控制功能。通常杀毒软件是无法查出它来的，请先确定该服务是否是自己开放并且是必需的。如果不是，可以关闭它。

打开命令提示符窗口，然后输入"cd C:\winnt\system32\r_server. exe /stop"命令后回车。

然后再输入"r_server /uninstall /silence"回车命令。

最后到 C:\winnt\system32 目录下删除 r_server. exe、admdll. dll、radbrv. dll 三个文件。

（4）5800、5900 端口

首先使用 fport 命令确定出监听在 5800 和 5900 端口的程序所在位置（通常是 c:\winnt\fonts\explorer. exe）。

然后在任务管理器中杀掉相关的进程（有一个是正常的系统进程，如果错杀可以重新运行 c:\winnt\explorer. exe）。

接着删除 c:\winnt\fonts\中的 explorer.exe 程序。

还要删除注册表 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 中的 Explorer 项。

最后重新启动机器。

(5) 6129 端口

6129 端口是一个远程控制软件(dameware nt utilities)服务端监听的端口,具有远程控制功能,通常的杀毒软件是无法查出它来的。请先确定该服务是否是自己安装并且是需要的,如果不是可以关闭。关闭 6129 端口方法如下。

在服务管理器中找到 DameWare Mini Remote Control 项右击选择属性,将启动类型改成禁用后停止该服务。

再到 c:\winnt\system32 目录下将 DWRCS.EXE 程序删除。

最后到注册表中将 HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\DWMRCS 项删除。

也可用"TCP/IP 筛选"来设置开始的端口,方法是在"本地连接"属性中选择"TCP/IP 协议"然后选择"属性",在打开的"常规"选项页中选择"高级",打开"选项"选项页,选择"TCP/IP 筛选"后选择"属性",在 TCP 端口上方选择"只允许",然后单击"添加"添加需要打开的端口,如上网必须要用的 80 端口。

#### 4. 卸载 WSH 功能

由于部分蠕虫病毒是采用 VBScript 脚本语言编写的,而 VBScript 代码必须由 WSH (Windows Script Host)解释执行。由于 WSH 一般不影响计算机的正常工作,所以,可以将 WSH 功能卸载掉,使蠕虫病毒失去出发运行的环境。具体方法如下。

要在 Windows 98 中删除 WSH,先打开"添加/删除"程序,选择"Windows 设置/附件"后单击"详细资料",取消 Windows Scripting Host 选项,然后单击"确定"按钮即可。

要在 Windows 2000/XP/Server 中删除 WSH,首先双击"我的电脑"图标,然后执行"工具/文件夹选项"命令,选择"文件类型"选项卡,选中 VBS VBScript Script File 选项,单击"删除"按钮,最后单击"确定"按钮即可。

另外,在操作系统上还要进行"删除 Guest 账号"、"限制不必要的用户数量"、"创建一个陷阱账号"操作,具体在第 4 章相关内容中已经详述。

### 6.3.3 防火墙

在黑客防范体系中,防火墙是特别重要的一种,是安全策略实施的核心要素。图 6-14 显示了一个用来分离不同网络区域的防火墙设备。各个功能区域通常也被称为安全区,这些区域包括专业区、公用区和非军事区(demilitarized zone,DMZ)。

Cisco 的《思科网络术语和缩略语词典》中对防火墙的定义是:"防火墙是在连接的公用网和专用网之间作为缓冲的路由器或接入服务器(一台或多台)。用作防火墙的路由器一般采用接入列表和一些其他方法来保证专用网的安全。"

如图 6-14 所示,防火墙的内部接口连接了一个专用的或者企业内联网,而外部接口则连接 Internet(不可信任网络),DMZ 是一个受隔离的网络,其中放置着 Web 服务器和

邮件服务器。

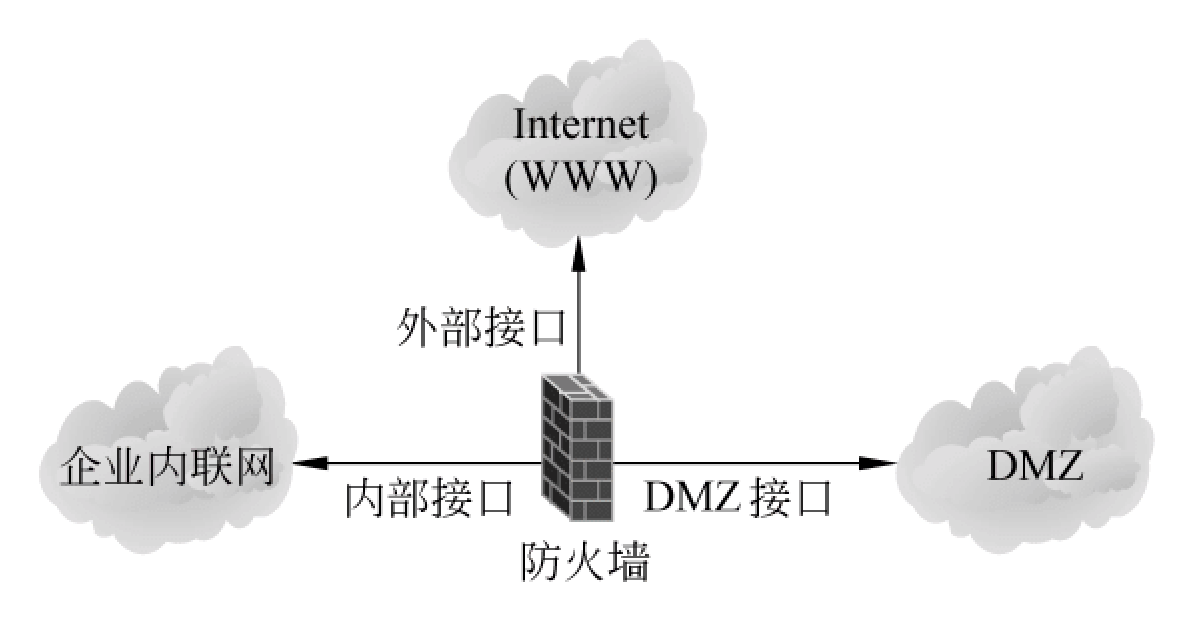



**图 6-14 防火墙部署**

防火墙通常是软件和硬件的组合体。它是基于被保护网络具有明确定义的边界和服务，并且网络安全的威胁大部分来自外部网络。它通过监测、限制以及更改跨越“防火墙”的数据流尽可能地对外部网络屏蔽有关被保护网络的信息、结构，实现对网络的安全保护。防火墙网络安全保障系统实施相当简单，是目前应用较广的网络安全技术，因为它把诸多安全功能集中到一点上，大大简化了安装、配置和管理的手续。另一个特点是它不限于 TCP/IP 协议，从而不只适用于 Internet，类似的技术完全可以用在任何分组交换网络当中，如 X.25 或 ATM 都可以。

图 6-15 是利用防火墙防范黑客在进行网络攻击前进行有关服务器信息收集的对策。

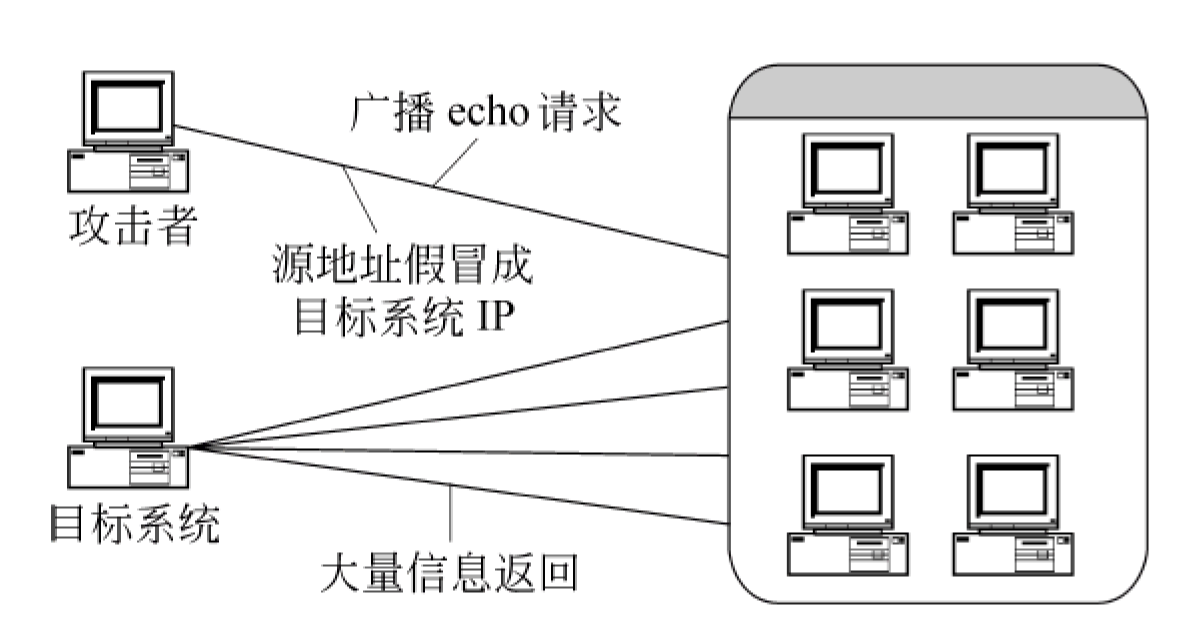



**图 6-15 利用防火墙防范黑客收集 DNS 信息**

在图 6-15 中可以看到，DNS 采用层次性分布，防火墙的 DMZ 和保护的网络中分别设置一台 DNS 服务器，在 DMZ 中的 DNS 服务器的区域分布文件中只需要定义公网上的服务器，而所有内部网络中的主机信息在内部 DNS 中定义，同时在防火墙上设置相应的规则，只允许外部网络访问 DMZ 中的 Web 和邮件服务器及 DNS 服务器，不允许对内部网络中的主机进行访问，但允许内部网络中的 DNS 服务器访问 DMZ 中的 DNS 服务器。也就是说内部网络中的主机需要访问外部网络时，通过 DMZ 中的服务器进行转发。同时设置防火墙不允许对 TCP 的 53 端口进行访问，因为一般的域名请求是通过 UDP 的 53 端口进行访问，而 TCP 53 的端口主要针对内部区域名服务器和外部域名服务器之间的区域文件进行传输。从上面可以看出很多信息安全的设置并不是单一的，而是通过功能不同的网络安全设备完成不同的任务。

有了防火墙设备，要设置好才会有效。一般防火墙安装后进入自定义 IP 规则进行设置，必须选择的有如下几点。

(1) 禁止互联网上的机器使用共享资源。

(2) 禁止所有人的连接。

(3) 禁止所有人连接 0～255 端口。

(4) 允许已经授权的程序打开端口。

这样一切需要开放的端口程序都需要审批,但是不要选择“系统设置”里的“允许所有应用程序访问网络,并在规则记录这些程序”。这个设置是防范反弹木马和键盘记录的秘密武器。

但是防火墙也不是坚不可摧的,其实防火墙也是一个专用的计算机系统,其本身也存在安全隐患,如果设置不当,也会留下漏洞,成为黑客攻击网络的桥梁。另外要特别注意的是防火墙只能防范外部网络的黑客攻击,而并不能防范内部网络的黑客攻击。具体有关防火墙的技术将在第 7 章中论述。

## 6.3.4 攻击检测

对于黑客攻击的防范,如果能够在黑客攻击的前期就能发现其行踪,阻断黑客攻击的过程,就会大大减少攻击造成的损失。目前,发现黑客攻击的手段一般采用网络攻击检测。网络攻击检测的基本假定前提是任何可检测的网络攻击都有异常行为,所以,网络攻击检测主要是检测网络中的异常行为。根据检测网络异常行为的不同方法、检测网络异常行为的不同位置,可以形成不同的攻击检测方案。

为了进行网络攻击的检测,必须能够描述网络攻击的特征。网络攻击包括了攻击者和受害者。从攻击者角度出发,网络攻击主要采用攻击的意图、攻击被暴露的危险程度等特征描述;从受害者角度出发,网络攻击主要采用攻击的显露程度、攻击可能造成的损失等特征描述。目前采用的攻击检测方法通常是从攻击者角度分析和研究网络攻击的特征。但是,为了有效部署和配置网络攻击检测系统,也需要从受害者角度出发分析网络攻击。

### 1. 典型网络攻击检测系统

网络攻击检测需要通过一个系统才能完成,首先需要对网络攻击检测系统有一个总体认识。典型的网络攻击检测系统如图 6-16 所示。

这个系统设置在企业网和公共 Internet 的连接部分,该系统采用了 2 个防火墙,设置了一个企业外部网和一个企业内部网。在企业网的外部网中连接了一个 WWW 服务器,在企业内部网通过网络交换设备连接了多台企业内部主机。整个系统包括了网络探测点、主机探测点、应用探测点、网络分析器、主机/应用分析器以及攻击检测控制台。

网络探测点分别设置在 Internet 段、企业外部网段和企业内部网段,用于提取可疑的数据传递给网络分析器。万维网服务器和主机执行主机探测点软件,监视外部与操作系统之间可疑的交互,提取可疑的交互数据传递给主机分析器。万维网服务器还执行应用探测点软件,监视对应用接口的可疑调用,并提取可疑的应用调用传递给应用分析器。

网络分析器和主机/应用分析器将分析结果提交给攻击检测控制台,确定对可疑事件的处理,例如,发布网络攻击警报、启动网络攻击防御系统、向网络安全管理员发送事

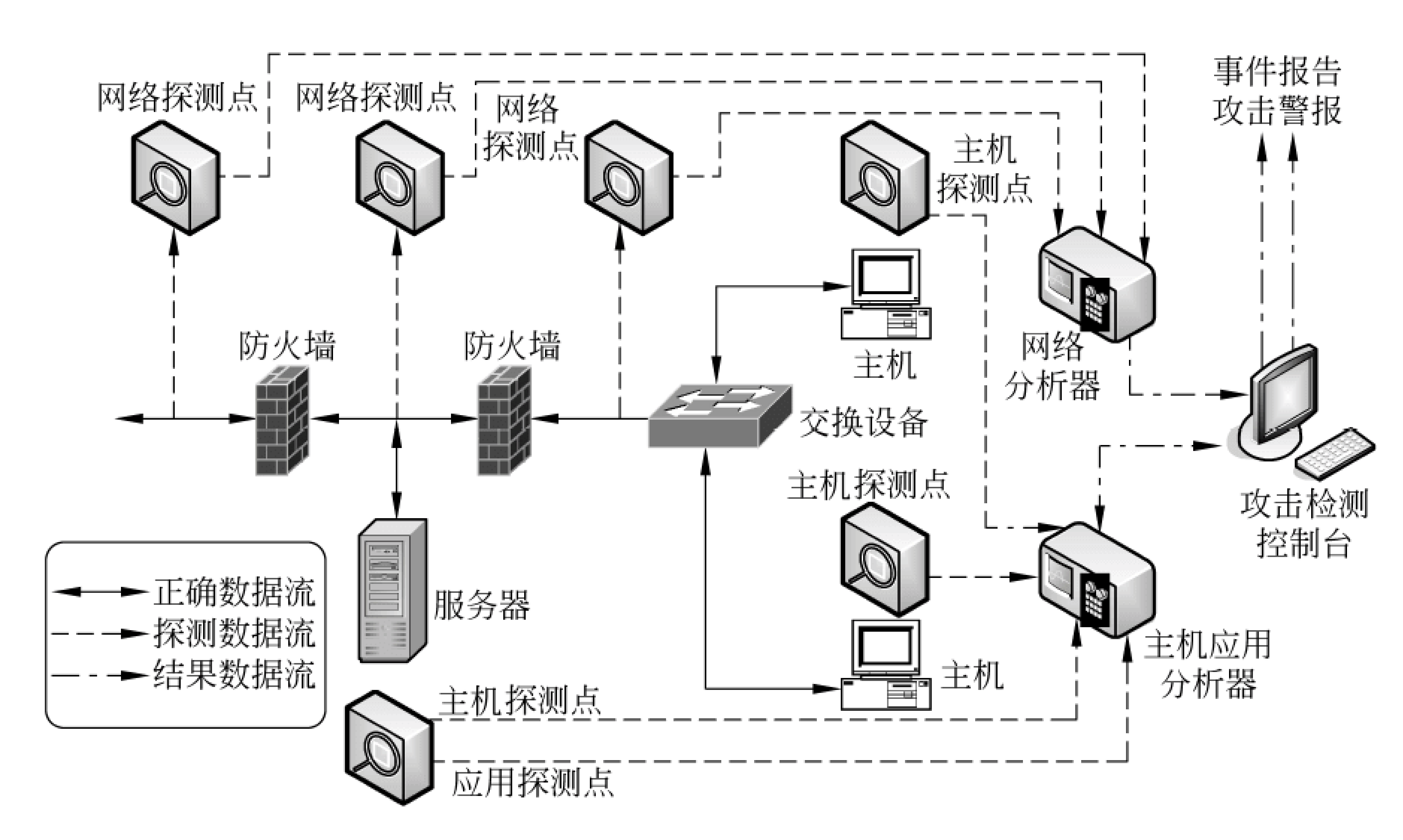



**图 6-16　一个典型的网络攻击检测系统结构**

件报告、向网络安全机构发送网络攻击报告等。

### 2. 网络攻击检测分类

网络攻击检测可以按照检测的对象不同进行分类,也可以按照检测的方法不同进行分类。从以上典型的网络攻击检测系统可以看出,网络攻击检测可以分为基于网络的攻击检测技术和基于主机的攻击检测技术。这是按照检测的对象不同而进行的分类,这也是从攻击检测系统的部署和使用角度对网络攻击检测的分类。

实际上网络攻击检测技术的本质区别在于检测的方法。所以,在对网络攻击检测的研究中,一般按照攻击检测的方法不同,将网络攻击检测分成特征检测方法和异常检测方法。

1）基于网络的攻击检测技术

基于网络的攻击检测技术是通过监视和分析网络上传递的一组可疑报文,检测网络上可能发生的或者正在发生的网络攻击的一类技术。基于网络的攻击检测设备一般部署在企业网多个关键的网段上,例如,典型攻击检测系统,基于网络的攻击探测点部署在连接企业网的公共 Internet 的网段、企业外部网的网段以及企业内部网的接入网段。

基于网络的攻击检测技术通过采集网络上传递的可疑报文,可以同时检测对多台主机的网络攻击。由于基于网络的攻击检测是实时攻击检测技术,要求网络探测点具有较高的分析和处理能力。如果在高速传输网段上探测可疑报文,将对攻击检测方法的性能提出很高的要求。这样,基于网络的攻击检测技术在高速网络环境下,会因为无法按照链路传递的速度探测报文而造成“漏报”的现象。

由于基于网络的攻击检测系统可以独立于网络设备和网络主机部署,不影响网络服务器和客户机的性能,易于配置和管理。所以,基于网络的攻击检测系统得到了较为广泛的应用。

2）基于主机的攻击检测技术

基于主机的攻击检测技术是通过检查计算机系统的日志数据和审核数据，以及监视应用与主机操作系统之间可疑的交互，检测可能发生的、正在发生的或者已经发生的网络攻击的一类技术。

基于主机的攻击检测技术可以检测某些针对主机的攻击，这些对网络主机的攻击是难以或者无法通过基于网络的攻击检测技术检测到的攻击。基于主机的攻击检测技术可以有效地检测一些特征不明显的攻击，例如，空耗系统资源、降低主机系统性能这类攻击。

基于主机的攻击检测技术需要在网络主机中安装和运行主机探测点软件和应用探测点软件，会在一定程度上影响网络主机的配置，降低网络主机的处理性能。另外，对于一些较为复杂的网络攻击，可以自动删除主机系统中与攻击相关的日志数据和审核数据，对基于主机的攻击检测造成一定的困难。所以，较为完整的攻击检测系统就像上面描述那个典型的攻击检测系统那样，通常综合了基于网络的攻击检测技术和基于主机的攻击检测技术。

3）网络攻击的特征检测方法

无论是基于网络的攻击检测技术，还是基于主机的攻击检测技术，都需要设计具体的攻击检测方法。网络攻击是网络系统中的非正常行为，所以，检测网络攻击也就是识别这些网络的非正常行为。

如果能够在分析已有的网络攻击的基础上，提取出网络攻击的特征模式，则可以通过对网络中正在发生的或者已经发生的行为进行模式匹配，找到可能发生的、正在发生的或者已经发生的网络攻击。这种网络攻击的检测方法就是特征检测方法。

网络攻击的特征检测方法的最大优点是对已经发现的网络攻击检测的精确度较高，它的最大缺点是无法检测到未知的网络攻击。另外，它与防病毒软件一样，需要不断更新、升级网络攻击特征库。

4）网络攻击的异常检测方法

为了有效地控制网络攻击造成的危害，必须能够及时检测到可能的网络攻击。这样，就要求攻击检测系统不能仅仅检测已经造成危害的网络攻击，必须能够及早发现可能的、新出现的网络攻击。这就需要从网络正常行为角度检测可能的网络攻击。

如果能够在正确地分析正常网络行为的基础上，建立一个正常网络行为的模式，则可以对网络上正在发生的和已经发生的行为进行分析、过滤，提取出非正常的网络行为，在进一步对非正常网络行为进行分析的基础上，检测出可能发生的、正在发生的或者已经发生的网络攻击行为。

网络攻击的异常检测方法主要优点是能够发现未知的、可能的网络攻击。它的主要不足是会将尚未描述的正常网络行为也作为网络攻击行为，造成较高的网络攻击的误报率，特别是在目前国际上还没有提出个完整的描述网络报文传递行为模型之前，很难建立一个通用的网络攻击的异常检测模型。但是在特定网络应用环境下的网络攻击异常检测方法还是可以取得较好的效果。

### 6.3.5 身份认证与安全密码

一般传统网络访问控制系统的用户认证采用用户名和密码组合方式或者 PIN 码，用安全术语来说，这些密码指的是可重用密码（reusable password）。这种系统已经用了好多年恐怕还要持续很多年。本节中会提到一些可重用密码的替代方案，因为这种机制并没有随着新技术和新工具的发展而有所更新。

**1. 安全密码**

可重用密码的弱点有很多。统计证明，许多用户倾向于使用弱密码。另外，经验告诉我们，用户很容易就会违背密码安全策略中定义的规则。例如，很多人习惯与他人共享密码，还有很多密码根本就没遵守密码安全策略。密码违背安全策略要求的情况包括：

（1）用户自行选择各种密码。

（2）违反密码长度要求。

（3）违反密码生命期要求。

（4）使用违规的字符和字母（大写、小写、数字和标点符号）。

密码或 PIN 码可以反复使用也是一个很大的问题，如果不考虑新技术的话，这个问题很难解决。

为了改进可重用密码的安全性，可以开发和实施更易于理解的标准和策略，使大家都具有对可重用密码弱点的意识。如今，有很多商业化的认证机制可作为补代方案，例如，挑战/响应和时间同步机制、令牌以及生物识别技术。下面的密码安全策略可作为计算机用户保护密码相关信息的最低要求。

（1）密码长度最少 8 个字符。

（2）字符类型为大写和小写字母。

（3）字符集包括数字、字母和特殊字符（如！ @ ＃ ＄ ％ˆ ＊ ()_＋ 之类）的组合。

（4）不要用字典或术语表中的单词。

（5）不能连续使用相同的字母（如 aaaa、88888 之类）。

（6）不要使用和个人信息相关的数字或词语（如姓名、生日、工作单位、住址、电话号码之类）。

（7）不要在不同的系统中使用相同的密码。

**2. 创建安全密码**

下面的方法可以用来创建一个比较容易记忆但又相对安全的密码。

（1）选择一个比较熟悉的英文单词，然后将其反转，然后在其前面或后面加一些比较熟悉的数字。比如选择 success，将其反为 sseccus ，在前面加上数字，比如 51168sseccus 等。

（2）在自己选择的密码组合中加上至少 1 个特殊字符（诸如 e ！ @ ＃ ＄ ％ˆ& ＊ ()_＋）。

（3）使用 1 个数字替代你所选择的作为密码的英文单词中的某个字母。比如，选择

international 作为自己的密码，然后用数字 3 代替单词中的 e，即使用 int3rnational 作为密码。

（4）在选中的英文单词中间隔加上数字。比如选择 security 作为基础，在每个字母之间加数字变成 s1e3c2u4r6i5t7y。

### 3. 如何记忆密码

对大多数用户而言，记住不同账号的不同密码是一件困难的事情，所以，他们常常懒得去记，或是把密码写下来，或是干脆找一个简单好记但非常容易被破解的密码。实际上，记忆密码并不是一件那么困难的事情，想想在自动提款机上取现金时，并没有太多的人感到自己的密码有多么复杂难记，因为他们深知这样才不至于损失钱财。如果每个用户对待自己或企业的敏感资料账户像对待自己的银行现金账户那样，他们也许就不会觉得记忆密码是那么困难的一件事情了。一般来说，记忆密码不一定要死记硬背，可以采用一些辅助方法。

1）联想法

在一个人的记忆过程中，联想常常发挥着很大的作用。在一个给定的时间段内，如果采用联想法帮助记忆，就能记住一些难记的电话号码。假如朋友的电话号码是 76898997，可以采用联想法："吃了不久不久就吃"，这样不费多大劲就可以记住了。记忆密码也是同样道理，比如，一个常与朋友保持联络的人可以给自己的邮件信箱创建密码为 59481say88（我就是不要说"拜拜"），这样有趣又方便。

2）解释法

例如，密码 Y13＃tiruceS 基本上由英文单词 security 反转而来（ytiruces），把反转后得到的字母第一个和最后一个字母大写，得到 YtiruceS，然后再把好朋友的生日日期放在第一个大写字母的后面，再加上一个特殊字符＃，这样就建立了一个自创的加密密码。

### 4. 身份认证

身份认证是网络安全系统中的第一道关卡，是网络安全技术的一个重要方面。身份认证机制限制非法用户访问网络资源，是其他安全机制的基础，是最基本的安全服务，其他的安全服务都要依赖于它。一旦身份认证系统被攻破，那么系统的所有安全措施将形同虚设。黑客攻击的目标往往就是身份认证系统。

身份认证一般可分为用户与主机间的认证和主机与主机之间的认证，其中用户与主机间的身份认证可以分为以下几种方式。

1）基于回调调制解调器的认证方式

这是一种维护系统有效用户表及其相应电话号码的设备。当用户拨号调用系统时，回调调制解调器获得用户的登录户头，挂起，再回头调用用户终端。这种方法的优点是，限制只有电话号码存于调制解调器中的人才是系统的用户，从而使非法侵入者不能从其家里调用系统并登录。这个方法的缺点是限制了用户的灵活性，并且仍需要密码，这是因为调制解调器不能仅从用户发出调用的地方唯一地标识用户。

2）基于 SSH 密码的认证方式

基于密码的认证方式是最常用的一种技术，但它存在严重的安全问题。它是一种单因素的认证，安全性仅依赖于密码，密码一旦泄露，用户即可被冒充。更严重的是用户往往选择简单、容易被猜测的密码，如与用户名相同、生日、单词等。这个问题往往成为安全系统最薄弱的突破口。密码一般是经过加密后存放在密码文件中，如果密码文件被窃取，那就可以进行离线的字典式攻击，这也是黑客最常用的手段之一。目前，人们在使用邮箱或留言板时所采用的密码是十分容易被破译的，尤其是 8 位数以下的数字，几乎用零点几秒就可以破译出来。另外，在一些个人的小网站上的留言板上发言时，发言密码不要使用和自己邮箱一样的密码。因为网站的管理员可以轻而易举地看到你的密码，如果网管缺乏职业道德就很有可能进入你的邮箱。

SSH 的英文全称是 Secure SHell。传统的网络服务程序，如 ftp、pop 和 telnet 在本质上都是不安全的，因为它们在网络上用明文传送密码和数据，别有用心的人非常容易就可以截获这些密码和数据。而且，这些服务程序的安全验证方式也是有弱点的，就是很容易受到“中间人”(man-in-the-middle)这种方式的攻击。“中间人”的攻击方式，就是“中间人”冒充真正的服务器接收你的传给服务器的数据，然后再冒充你把数据传给真正的服务器。服务器和你之间的数据传送被“中间人”一转手做了手脚之后，就会出现很严重的问题。通过使用 SSH，你可以把所有传输的数据进行加密，这样“中间人”这种攻击方式就不可能实现了，而且也能够防止 DNS 和 IP 欺骗。

SSH 密码(passphrase)是使用一个短语或者一句话作为密码输入，由系统内部的加密或是散列算法生成虚拟密码(virtual password)后，进行下一步的认证。这种技术的优越之处是容易记忆，不易被破解，通常人们设置 SSH 密码时都使用一些自己永远记得或常常惦记的事物，可以是一句话，也可以是一组数字或特殊字符，比如 ilovemymother。尽管由于 SSH 密码的长度使得攻击者破解起来非常困难，但是如果登录的设备上安装了 keylogger 之类的键盘记录器，那么，多长的 SSH 密码也会被记录下来。

3）一次性密码认证方式

简单的认证中只有名字和密码被服务系统所接受。由于明文的密码在网上传输极容易被窃听截取，一般的解决办法是使用一次性密码(one-time password，OTP)机制。这种机制的最大优势是无须在网上传输用户的真实密码，并且由于具有一次性的特点，可以有效防止重放攻击(replay attack)。根据一次性密码生成机制的不同，通常 OTP 可分为 Time Synchronization 的 Secure ID(安全标识符)、Challenge-Response 的 Crypto Card(密码卡)和增强的 S/Key(安全密钥)等。

OTP 的主要思路是在登录过程中加入不确定因素，使每次登录过程中传送的信息都不相同，以提高登录过程安全性。例如，登录密码＝MD5(用户名＋密码＋时间)，系统接收到登录密码后做一个验算即可验证用户的合法性。确定因子选择方式大致有以下几种。

(1) 密码序列(S/KEY)密码：为一个单向的前后相关的序列，系统只用记录第 N 个密码。用户用第 N－1 个密码登录时，系统用单向算法算出第 N 个密码与自己保存的第 N 个密码匹配，以判断用户的合法性。由于 N 是有限的，用户登录 N 次后必须重新初始

化密码序列。

(2) 挑战/回答(CRYPTOCard):用户要求登录时,系统产生一个随机数发送给用户。用户用某种单向算法将自己的秘密密码和随机数混合起来发送给系统,系统用同样的方法做验算即可验证用户身份。

(3) 时间同步(secureID):以用户登录时间作为随机因素,这种方式对双方的时间准确度要求较高,一般采取以分钟为时间单位的折中办法。在SecureID产品中,对时间误差的容忍可达±1分钟。

(4) 事件同步(safe word):这种方法以挑战/回答方式为基础,将单向的前后相关序列作为系统的挑战信息,以节省用户每次输入挑战信息的麻烦。但当用户的挑战序列与服务器产生偏差后,需要重新同步。

一次性密码的生成方式有以下几种。

(1) Token Card(硬件卡):用类似计算器的小卡片计算一次性密码。对于挑战/回答方式,该卡片配备有数字按键,便于输入挑战值;对于时间同步方式,该卡片每隔一段时间就会重新计算密码;有时还会将卡片作成钥匙链式的形状,某些卡片还带有PIN保护装置。

(2) Soft Token(软件):用软件代替硬件,某些软件还能够限定用户登录的地点。

(3) IC卡:在IC卡上存储用户的秘密信息,这样用户在登录时就不用记忆自己的秘密密码了。

4) 基于智能卡的认证方式

智能卡具有硬件加密功能,有较高的安全性。每个用户持有一张智能卡,智能卡存储用户个性化的秘密信息,同时在验证服务器中也存放该秘密信息。进行认证时,用户输入PIN(个人身份识别码),智能卡认证PIN成功后,即可读出智能卡中的秘密信息,进而利用该秘密信息与主机之间进行认证。基于智能卡的认证方式是一种双因素的认证方式(PIN+智能卡),即使PIN或智能卡被窃取,用户仍不会被冒充。智能卡提供硬件保护措施和加密算法,可以利用这些功能加强安全性能,例如,可以把智能卡设置成用户只能得到加密后的某个秘密信息,从而防止秘密信息的泄露。

5) 基于生物特征的认证方式

这种认证方式是以人体唯一的、可靠的、稳定的生物特征(如指纹、虹膜、脸部、掌纹等)为依据,采用计算机的强大功能和网络技术进行图像处理和模式识别。基于生物特征识别的身份鉴定技术具有以下优点:不易遗忘或丢失;防伪性能好,不易伪造或被盗;随身携带,随时随地可用。该技术具有很好的安全性、可靠性和有效性,与传统的身份确认手段相比,无疑产生了质的飞跃。近几年来,全球的生物识别技术已从研究阶段转向应用阶段,使生物识别技术的应用即将成为可能。目前,国外许多高技术公司正在试图用眼睛虹膜、指纹、面貌特征等取代人们手中的信用卡或密码,并且已经开始在机场、银行和各种电子器具上进行了实际应用。

更加详细的身份认证系统将在第7章论述。

## 6.3.6 内部管理

为了对付内部产生的黑客攻击要在安全管理方面采取措施。世界头号黑客凯文·米特尼克曾经说:“不要太过于将注意力集中在技术防护,其实人是最容易出问题的因素。”黑客一般最喜欢的伎俩是采用一些技术手段,骗取他人的信任,轻松获取甚至用户会自动奉送密码以及机密软件代码。如果管理人员疏于遵守安全措施,再好的安全设备也是形同虚设。所以,成功安全防范体系应该是在技术手段的基础上,关注网络管理人员的因素,加强内部管理。

**1. 慎重选择网络系统管理员**

必须慎重选择网络系统管理人员,对新职员的背景进行调查,网络管理等要害岗位人员调动时要采取相应防护措施(如及时更改密码)。

网络管理人员要有高度的责任心,有足够的安全意识随时提高警惕不要轻易相信自己的系统安全已经是万无一失。网络运行时,要严密监视网络,判断哪些信息是用户的,哪些信息不是用户的。一旦发现正受到攻击,要及时防范减少不必要的损失。从某种意义上说,网络安全与网络系统管理员的责任具有密切的联系。

**2. 制定详细的安全管理制度**

确保每个职员都了解安全管理制度,如掌握正确设置较复杂密码的要求,分清各岗位的职责,有关岗位之间要能互相制约,及时更新系统补丁和杀毒软件。

**3. 签订法律文书**

企业与员工签订著作权转让合同,使有关文件资料、软件著作权和其他附属资产权归企业所有,以避免日后无法用法律保护企业利益不受内部员工非法侵害。

**4. 安全等级划分**

将部门内电子邮件资料及 Internet 网址划分保密等级,依据等级高低采取相应的安全措施及给予不同的权限。

**5. 定期改变密码**

永远不要对自己的密码过于自信,也许就在无意当中泄露了密码。定期改变密码,会使自己遭受黑客攻击的风险降到一定限度之内。一旦发现自己的密码不能进入计算机系统,应立即向系统管理员报告,由管理员来检查原因。系统管理员也应定期运行一些破译密码的工具来尝试,若有用户密码密码被破译出,说明用户的密码设置过于简单或有规律可循,应尽快地通知他们及时更改密码。

**6. 加强技术上的管理**

俗话说得好“没有不透风的墙”,而且黑客还可直接利用 80 端口进行攻击或利用一

些还不为我们所知的漏洞进行攻击。但黑客入侵电脑肯定会留下踪迹，那又如何查到他们留下的蛛丝马迹呢？

1）启动审核策略

进入“控制面板”，打开“管理工具”，再打开“本地安全设置”，选择“安全设置”下“本地策略”中的“审核策略”，双击“审核登录事件”和“审核对象访问”，将“成功”和“失败”都勾选上，这样就开启了事件记录，以后只要有关于登录的事件都会被记录在日志中（如记下对方的 IP 甚至用户名）。但这些日志文件主要是 c:\winnt 和 c:\winnt\system32\目录下的 txt 文件和 log 文件，还有 c:\winnt\system32 下 logfiles 中的所有文件，config\下的 evt 文件和 dtclog 下的所有文件。如果黑客把这些文件删除，那么在日志中就看不见任何东西了。当然如果日志里忽然任何内容都没有了那一定是被入侵了。

2）检查开放的端口和利用嗅探器监视网络通信

远程控制型木马以及输出 shell 型木马大都会在系统中监听某个端口，接收从控制端发来的命令并执行。通过检查系统上开启的一些“奇怪”的端口（如冰河木马默认端口为 7626），从而发现木马的踪迹。常用的软件有 Fport 和 Aport，它们可列出本地计算机所开的端口及开启端口的程序。如果还想了解黑客的 IP，甚至账号、密码和邮箱，可安装嗅探器（sniffer）或网络检测工具 Tcpview. exe。可以直接查看并中断任一通信进程。也可在 CMD 里输入“Sniffer-pass-log mail. txt”，就是截取所有密码放置在 Mail. txt，就可以直接查看这个文件得到较为详细的情报。

3）检查注册表

木马为了能在开机后自动运行，往往在注册表如下位置中添加注册表项。

HKEY_CURRENT_USER\Software\Microsoft\Windows\Currentversion\Run\Runonce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Currentversion\Run\runonce

HKEY_USERS\. Default\Software\Microsoft\Windows\Currentversion\Run

如果在以上项里发现有些程序文件不是用户安装的，那就很有可能中了木马。在 Windows 98 系统中，木马会在 win. ini 和 system. ini 的“run=”、“load=”、“shell=”后加入自己的程序名，而且有些木马程序与正常的文件程序很相似，不仔细观察很难发现。也有些木马会在系统进程中留下足迹，甚至将自己作为服务添加到系统中，或随机替换系统中没启动的服务程序来实现自加载，这就需要对操作系统的常规进程和服务有所了解。

4）手工删除木马和蠕虫病毒

当发现可疑文件时，最直接的方法就是运行防毒软件（最好是利用实时监控进来一个杀一个）。好的杀毒软件不仅能杀掉一些著名的病毒，还能查杀大量的木马程序。这样，那些黑客们使用的有名的木马（如冰河、灰鸽子、广外女生）就毫无用武之地。不过不要忘了经常升级病毒库。还有就是利用查杀木马软件木马克星和 360 安全卫士。

但新木马的产生总是会在杀木马软件之前，这就需要进行手工删除。对于查到的可疑文件不能立即删除，因为只是可疑而已（而且有的木马是依附在某些文件上的）。首先

要备份可疑文件和注册表(可直接在注册表编辑器中的“注册表”菜单中“导出注册表文件”进行备份)。对于可疑文件可通过 ULTRAEDIT32 编辑器查看文件首部信息,通过可疑文件里的明文字符对木马有一大致了解,最后删除“木马”文件及注册表中的键值,如提示文件正在运行无法删除,则重启进入安全模式再删。

如果杀毒软件不能清除蠕虫病毒,就只能根据蠕虫病毒的工作机理手工清除了,当然这种方法要求用户具有较高的计算机方面的知识与技能。首先,要根据蠕虫病毒利用的漏洞类型给系统打相应的补丁,以免计算机再次遭受蠕虫的攻击。其次,打开任务管理器根据蠕虫病毒的名称查找病毒进程,找到后直接结束该进程。由于蠕虫病毒为了每次计算机重启后都能获得计算机的控制权,所以,进入计算机的蠕虫病毒会修改计算机的注册表,并建立自己的注册表项,所以,要删除该病毒的注册表项。最后,根据注册表提供的信息找到病毒文件并删除。

另外,对于 Windows 98 用户的安全管理可以通过加强用户登录的安全性、使用用户自定义的桌面配置和实施用户策略来实现。

5) ARP 欺骗的防御

针对 ARP 欺骗的方法和危害,初步的防御方法如下:

(1) 不要把网络安全信任关系建立在 IP 地址的基础上或硬件 MAC 地址基础上,(RARP 同样存在欺骗的问题),理想的关系应该建立在 IP+MAC 基础上。

(2) 设置静态的 MAC 与 IP 对应表,不要让主机刷新设定好的转换表。

(3) 除非很有必要,否则停止使用 ARP,将 ARP 作为永久条目保存在对应表中。在 Linux 下可以用 ifconfig-arp 可以使网卡驱动程序停止使用 ARP。

(4) 使用代理网关发送外出的通信。

(5) 修改系统拒收 ICMP 重定向报文。

(6) 在 Linux 下可以通过在防火墙上拒绝 ICMP 重定向报文或是修改内核选项重新编译内核来拒绝接收 ICMP 重定向报文。

(7) 在 Windows 2000 下可以通过防火墙和 IP 策略拒绝接收 ICMP 报文。

### 6.3.7 个人计算机系统安全

个人计算机系统的安全是网络安全保障的重要组成部分,每个计算机用户对自己使用的计算机系统除了常规的系统安全措施,如启用操作系统自带的防火墙、启用自动更新功能、打补丁、安装并经常更新杀病毒软件(千万不要同时启用两套以上的杀病毒软件)、安装杀木马软件以及养成良好上网习惯以外,还应注意以下方面。

#### 1. 密码安全

计算机用户在选取密码时应尽量避免使用不安全的密码,要选择不易被破解的安全的密码。容易选择而且又缺乏安全性的密码包括以下几种。

(1) 使用与用户名相同的密码,或使用用户名的变换形式作密码。这样做的优点就在于密码不容易遗忘,但它的缺点也很明显,这是一个典型的“弱密码”。

(2) 使用生日作为密码。很多用户为了便于记忆选择 6~8 位的生日作为密码,看起

来有 1 000 000 或 100 000 000 种不同的选择,但事实上,考虑到年份的选择一般只是 19 开头,而月份只有 12 种选择,日期的选择也只有 31 种,所以可以选择的密码只有 12×31×100=37200 种。如果再考虑到实际使用计算机的用户的年龄限制,比如从 10～70 岁,那么这种密码的选择基数会更小,搜索的时间可以更短。

(3) 使用常用的英文单词作为密码。

(4) 使用较短的字符串作为密码,比如选择 8 位以下的字符串作密码。

要选择安全有效的密码,应该遵循以下规则。

(1) 选择长的密码,密码越长,黑客猜中的可能性就越低。

(2) 最好的密码包括大小写英文字母和数字的组合,比如 SB6xgz7v。

(3) 定期更换密码。原则上,所有的密码都是可能被破解,只是所费时间的长短不同而已。所以,一个相对安全的密码要配上 3～6 个月更换一次的安全制度才是真正安全的。

另外在使用密码的过程中要注意以下事项。

(1) 不要将密码写下来,或存放于存储器中。

(2) 不要在不同系统上使用同一个密码。

(3) 不要让其他人看见自己输入密码。

(4) 如果密码在网上传输,则应对密码加密或在系统中安装相关软件或硬件来使用一次性密码。

### 2. QQ 的安全

QQ 是国内最成功的即时通信软件,其合理的设计、良好的易用性、强大的功能和稳定高效的系统运行,赢得了用户的青睐。QQ 用户群已成为中国最大的互联网注册用户群。作为一种即时工具,QQ 采用的是 C/S 模型,使用的是 UDP 协议。和 TCP 相比,UDP 本身是不可靠的,可被轻易地伪造。使用 TCP 的软件必须自身在两端进行可靠性检测。但和 TCP 相比,UDP 资源占用小,这也是 QQ 选择 UDP 的主要原因。在 QQ 的传输中,数据是以明文的形式发送的,也就是说,一个窃听者能直接偷听到经过他的所有 QQ 信息。所以,虽然 QQ 功能实用不花哨,但在安全性方面还有很多需要用户警惕之处。下面介绍几种常见的 QQ 攻击和防御方法。

1) 在 QQ 中显示对方的 IP 地址

虽然严格意义上讲,在 QQ 中显示对方的 IP 地址并不算黑客攻击,但是通过获得对方的 IP 地址,可为进一步的攻击(比如 QQ 消息炸弹)做准备。所以,在使用 QQ 时应尽量避免 IP 地址和端口号泄露。具体的安全建议如下：在 QQ 的个人设置里修改身份默认值为“需要身份验证才能把我加为好友”,在 QQ 参数设置中,选择“拒绝陌生人消息”,这样可以避免与攻击者进行直接通信。通过代理服务器上 QQ 或隐身登录 QQ。通过代理服务器上 QQ,可以隐藏自己的 IP 地址,而攻击者所看到的 IP 地址只是代理服务器的 IP 地址。隐身登录 QQ 后发送的消息是通过 QQ 服务器中转的,这样,攻击者只能获得 QQ 服务器的 IP 地址。使用一些隐藏 IP 地址的工具软件把 IP 地址隐藏起来,比如,使用天网个人防火墙来防止外部计算机探测本机 IP 地址。

2）QQ 密码破解

QQ 密码的破解方法分为在线破解和非在线破解。在线破解是指到 QQ 的验证服务器中直接破解密码，其他破解方法都统称为非在线破解。破解 QQ 密码最常用和有效的方法就是在线破解 QQ 密码。在线破解的工具有很多，其中 QQPH 在线破解大王、天空葵 QQ 密码探索者和 QQExplorer 是三个最有名的工具，并称为三大 QQ 扫号工具。这三个 QQ 扫号工具在许多黑客网站都可以下载，除了拥有界面友好和操作方便的特点之外，还有一大共同的特点就是都使用密码穷举法来猜测密码。如果在 QQ 密码在线破解工具的密码字典中没有某个 QQ 号的正确密码，那么这个 QQ 号码的密码就不会被扫描到，所以针对 QQ 在线密码破解安全建议如下：

（1）注意 QQ 密码的长度和复杂性，设置一个长的复杂的密码将会使破解的难度大大增强。

（2）到腾讯的网站申请密码保护。为了防止 QQ 密码被破解，QQ 号码被盗用，腾讯提供了 QQ 密码的保护，网址为 http://service.tencent.com/reg/register.shtml。

多数的 QQ 密码是在本机被攻破的，进行 QQ 密码非在线破解的工具同样也有很多，比如密码瞬间破解器和 QQ 木马程序。针对 QQ 非在线密码破解的安全建议如下：

（1）登录 QQ 时，不要让计算机记住密码，也不要在 QQ 系统参数设置中选择“不出现登录提示框”。

（2）在公共场合使用 QQ 后，要删除以 QQ 号为名的文件夹或立即更改自己的 QQ 密码。

（3）使用木马查杀工具来消除计算机中的 QQ 木马程序。

3）QQ 消息炸弹

这种攻击就是向远程的在线 QQ 用户自动发送大量的消息，从而使远程的 QQ 用户疲于应付这些消息，无法进行正常 QQ 操作的攻击方法。这种攻击方法主要有两种形式：一种是在对话模式中，利用工具软件向对方发送消息炸弹；另一种是指定远程 QQ 用户对应的 IP 地址和端口号，然后利用工具软件发送消息炸弹。这主要是利用 UDP 数据通信不需要验证确认的弱点，只要拿到用户的 IP 地址和 QQ 通信端口即可发动攻击。针对 QQ 消息炸弹的安全建议如下：

（1）在 QQ 的个人设置中设置“需要身份验证才能把我加为好友”，以防止陌生人的攻击。

（2）若是来自好友的“轰炸”，应按下 Ctrl＋Alt＋Del 组合键杀死 QQ 进程，并将恶意好友删除。

（3）在 QQ 参数设置中，选择“拒绝陌生人消息”，这样可以避免被垃圾信息所骚扰。

### 3. 电子邮件的安全

随着网络的普及，几乎每个上网的人都拥有一个或一个以上的邮箱，电子邮箱正成为人们工作和生活中不可缺少的一部分。对于电子邮件的攻击主要有电子邮箱的密码破解与电子邮件炸弹两种。有很多工具能窃取电子邮箱的密码，如 Emailcrack、黑雨 POP3 邮箱密码暴力破解器、溯雪 Web 探测器和流光等。这些电子邮箱的入侵实际上都

是一种密码破解攻击方法。所以,对于这种攻击的防御就是按前述密码安全中所描述的方法选择安全的密码即可。电子邮件炸弹,英文是 E-mail Bomb,它是指那些自身体积(字节数)超过了信箱容量的电子邮件,或者由服务器短时间内连续不断地向同一个信箱发送大量的电子邮件。邮件炸弹可以说是目前网络中很"流行"的一种恶作剧。当某人所作所为引起了好事者不满时,好事者就可以通过这种手段来发动进攻。这种攻击手段不仅会干扰用户的电子邮件系统的正常使用,甚至它还能影响到邮件系统所在的服务器系统的安全,造成整个网络系统全部瘫痪,所以,邮件炸弹也有很大的危害。

邮件炸弹可以大量消耗网络资源,常常导致网络堵塞,使大量的用户不能正常地工作。通常网络用户的信箱容量是很有限的,在有限的空间中,如果用户在短时间内收到成千上万封电子邮件,那么经过一轮邮件炸弹轰炸后的电子邮件的总容量就把用户有限的阵地挤垮。导致用户的邮箱中将没有多余的空间接纳新邮件,新邮件将会被丢失或者被退回,使得用户的邮箱失去作用。另外,邮件炸弹所携带的大容量信息不断在网络上来回传输,很容易堵塞带宽并不富裕的传输信道,这样会加重服务器的工作强度,减缓了处理其他用户的电子邮件的速度,从而导致了整个过程的延迟。现在,已经有很多种能自动产生邮件炸弹的软件程序,如 Kaboom! 邮件炸弹或 Haktek 邮件炸弹。

要防范邮件炸弹的攻击,首先不要将自己的邮箱地址到处传播,且最好用 POP3 收信。可以用 Outlook Express 或 Fox mail 等 POP3 收信工具收取邮件。以 Outlook Express 为例,可以选择"工具→邮件规则→邮件",在弹出的"新建邮件规则"窗口中对符合条件的邮件设置处理方式。若想过滤超过 1024KB 的邮件,可以在上述的窗口中的"1. 选择规则条件"里选择"若邮件长度大于指定的大小",在"2. 选择规则操作"里选择"从服务器上删除",如图 6-17 所示,然后在"3. 规则描述"里单击"指定的大小",在弹出的窗口中输入 1024 后如图 6-18 所示,单击"确定"按钮,再分别单击"新建邮件规则"窗口和"邮件规则"窗口的"确定"按钮即可。




图 6-17 Outlook Express 新建邮件规则窗口




图 6-18 设置接收邮件大小的窗口

当有人不停攻击一个邮箱时,可以先打开一封信,查看对方地址,然后在收件工具的过滤器中选择不再接收来自这个地址的信,直接从服务器上删除。

在收邮件时,一旦看见邮件列表的数量超过平时正常数量的若干倍,应当马上停止下载邮件,然后从服务器删除炸弹邮件。可以使用“砍信机”工具或 E-mail chomper 等软件,帮助用户快速删除炸弹邮件。另外,一旦被 E-mail 炸弹攻击,可以马上通知邮件服务器的管理员,请他删掉炸弹邮件。

安装电子邮件过滤器也能有效地阻止电子邮件的攻击。现在大多数电子邮件服务器已带有邮件过滤功能。

### 4. 修改注册码防范黑客程序

病毒、木马、后门以及黑客这些程序感染计算机的一个共同特点是在注册表中写入信息,来达到如自动运行、破坏和传播等目的。通过修改注册表来对付病毒、木马、后门以及黑客程序,保证个人计算机的安全。以下是修改注册表防御常见木马攻击的方法。

1) 预防 Acid Battery v1.0 木马的破坏

若在 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices 下右边窗口中发现了 Explorer 键值,则说明中了 Acid Battery 木马,将它删除。

2) 预防 YAI 木马的破坏

若在 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices 下右边窗口中发现了 Batterieanzeige 键值,则说明中了 YAI 木马,将它删除。

3) 预防 Eclipse 2000 木马的破坏

若在 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices 下右边窗口中发现了 bybt 键值,将它删除,然后在 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices 下删除右边的 cksys 键值,重新启动电脑。

4) 预防 BO2000 的破坏

若在 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices 下右边窗口中发现了 umgr32.exe 键值,则说明中了 BO2000,将它删除。

5) 预防爱虫的破坏

若在 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 下右边窗口中发现了 MSKernel32 键值,将它删除。

6) 禁止出现 IE 菜单中“工具”栏里“internet 选项”

把 c:\windows\system 下的 inetcpl.cpl 文件更名为 inetcpl.old 或别的名字,会出现禁止使用的情况。再把名字换回来,就可以恢复使用了。

7) 预防 BackDoor 的破坏

如在 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 下右边窗口中发现了 Notepad 键值,将它删除。

8）预防 WinNuke 的破坏

在 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\MSTCP 下右边窗口中新建或修改字符串 BSDUrgent，设其值为 0。

9）预防 KeyboardGhost 的破坏

如在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices 下发现 KG.EXE 这一键值，将它删除。查找 KG.exe 文件和 kg.dat 文件，将它们都删除。

10）查找 NetSpy 黑客程序

在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 下右边窗口中寻找 NetSpy 键。如果存在，就说明已经装了 NetSpy 黑客程序，把它删除。

11）清理访问“网上邻居”后留下的字句信息

在 HEKY_CURRENT_USER/Network/Recent 下删除里面的主键。

12）取消登录时自动拨号

在 HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Network/RealModeNet 下修改右边窗口中的 autologon 键值为 01 00 00 00 00。

13）取消登录时选择用户

已经删除了所有用户，但登录时还要选择用户。要取消登录时选择用户，就要在 HKEY_LOCAL_MACHINE\Network\Logon 下右边窗口中修改 UserProfiles 键值为 0。

14）隐藏上机用户登录的名字

在 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon 下右边窗口中新建字符串 DontDisplayLastUserName，设值为 1。

目前，黑客攻击对网络安全的威胁已经成为最主要的形式，本章首先对黑客的类型、行为特征、黑客攻击的目的、黑客的攻击过程以及攻击方式做了较为详细的论述。在此基础上对黑客进行网络攻击所采用的主要的技术手段，如端口攻击、漏洞攻击、网络监听、密码攻击、木马攻击、病毒与蠕虫攻击、缓存溢出攻击以及常见的其他攻击手段，在原理、实施的方式以及攻击实施的过程都进行了详细的分析。从上述的论述中可以知道，黑客是利用网络存在的各种漏洞和缺陷进行全方位攻击的，因此，对黑客的防范也必须从网络安全整体防范的角度出发，主要是堵住漏洞，包括网络设备、网络应用服务器的操作系统方面的漏洞，再结合主动防范意识，部署防火墙、攻击检测以及身份认证系统，加强内部管理，同时注意加强个人用户的安全行为的培养，如注意保护自己的密码，保护自己的计算机操作系统的安全。这样才能够在与黑客的对抗中处于相对的主动地位。

## 习　题　6

（1）什么是黑客？通常有哪几种类型？

（2）黑客的攻击方式有哪些？

(3) 黑客攻击的过程有哪些？其作用是什么？
(4) 有哪些端口是黑客攻击经常采用的？如何采取措施？
(5) 密码攻击是如何进行的？如何在日常工作中保证密码安全？
(6) 网络监听的原理是什么？其目的是什么？
(7) 木马的工作原理是什么？它有什么特征？
(8) 如何通过修改注册表来达到防范木马程序的目的？
(9) 蠕虫与病毒的区别是什么？如何防范蠕虫攻击？
(10) 参考1.2.4节，说明缓存溢出的原理是什么？如何防止出现缓存溢出攻击？
(11) 拒绝服务攻击有哪几种主要类型？
(12) 个人用户应该在哪几方面注意黑客攻击？

# 第 7 章 chapter 7

# 网络安全系统

建立一个安全的网络，需要从多方面入手，要加强主机本身的安全，减少漏洞；要用系统漏洞检测软件定期对网络内部系统下扫描分析，找出可能存在的安全隐患；要建立完善的访问控制措施，安装防火墙，加强授权管理和认证；要在线监控非法入侵和异常行为，实时报警和切断非法行为；要加强数据备份、容灾和数据恢复措施；要对敏感的设备和数据建立隔离措施；要在公共网络上传输敏感数据要用专用信道和加密；要加强内部网的整体防病毒措施；要建立详细的安全日志审计等。

本章将对上述涉及的技术和安全设备在基本工作原理、类型、选购因素和配置进行详细的论述。

## 7.1 防 火 墙

防火墙是指设置在不同网络（如可信任的企业内部网和不可信的公共网）或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口，通过监测、限制、更改跨越防火墙的数据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况，有选择地接受外部访问，对内部强化设备监管、控制对服务器与外部网络的访问，通过在被保护网络和外部网络之间架起一道屏障，来防止发生不可预测的、潜在的破坏性侵入。因此，对用户来讲，防火墙一般是部署在公共的不可信的互联网与用户可信的内部网之间，比较好的是进一步把用户的内部网用防火墙分隔为用户外部网（非军事区 DMZ）和用户内部网，其中用户外部网主要用于提供给外部访问的服务器，而内部网主要是提供给内部访问的服务器，部署原理如图 7-1 所示。

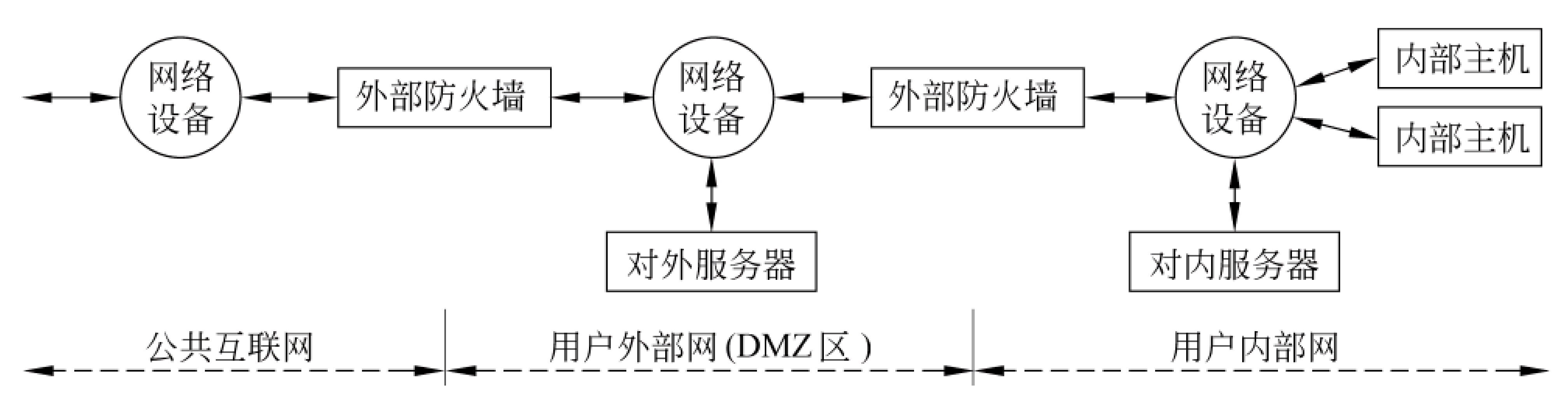



**图 7-1 防火墙应用的典型部署**

防火墙有硬件防火墙和软件防火墙两种，它们都能起到保护作用并筛选出网络上的攻击者。而对于企业网络环境的实际应用来说，更为常见的是拥有更全面、更高效、更完整的安全性能的硬件防火墙。

## 7.1.1 防火墙概述

### 1. 防火墙原理

防火墙常用的安全控制手段主要有包过滤、状态检测、代理服务。透明且传输性能高的包过滤技术是一种简单、有效的安全控制技术。包过滤技术通过在网络间相互连接的设备上加载允许、禁止来自某些特定的源地址、目的地址、TCP 端口号等规则，对通过设备的数据包进行检查，限制数据包进出内部网络。由于安全控制层次在网络层和传输层，安全控制的力度也只限于源地址、目的地址和端口号，因而只能进行较为初步的安全控制，对于恶意的拥塞攻击、内存覆盖攻击或病毒等高层次的攻击手段，则无能为力。

状态检测是比包过滤更为有效的安全控制方法。对新建的应用连接，状态检测检查预先设置的安全规则，允许符合规则的连接通过，并在内存中记录下该连接的相关信息，生成状态表。对该连接的后续数据包，只要符合状态表，就可以通过。由于采用了记录生成状态表的做法，检测时可直接通过散列算法检测后续数据包，使性能得到较大提高，加上状态表是动态的，因而可以有选择地、动态地开通 1024 号以上的端口，使得安全性得到进一步地提高。

### 2. 使用防火墙的意义

当机构的内部数据和网络设施暴露给 Internet 上的黑客时，网络管理员越来越关心网络的安全。为了提供所需级别的保护，机构需要有安全策略来防止非法用户访问内部网络上的资源和非法向外传递内部信息。即使一个机构没有连接到 Internet 上，它也需要建立内部的安全策略来管理用户对部分网络的访问，并对敏感或秘密数据提供保护。如果没有防火墙的话，可能会接到许许多多类似的报告。例如，公司的内部财政报告刚刚被发向 2 万个 E-mail 地址，或者主页被人链接到了 Playboy，而销售报告链接却指向了 Penthouse。如果内部网络联入了互联网的话，最好提前考虑这些问题，黑客可能会攻击任何感兴趣的系统。现在随着电子商务和网上交易的快速增长，保障信息的机密性、完整性、可用性和可控性就是至关重要的，而防火墙就是一个比较好的解决方案。但是防火墙不可能做到万无一失，它不是解决所有网络安全问题的万能药方，只是网络安全政策和策略中的一个组成部分，没有任何一种防火墙可以达到绝对的保护。构筑防火墙的目的也只是加强安全比而不是保证安全。并且防火墙也只是一种工具，只有根据安全策略加以初始化才能够真正起作用。况且任何防火墙都是由人来管理的，对于一个经常忘记锁门的人来说，给他再厚的墙也没有用。

### 3. 使用防火墙的好处

在没有防火墙时，内部网络上的每个节点都会暴露给外部网络上的其他主机，极易

受到攻击。这就意味着内部网络的安全性要由每一个主机的坚固程度来决定，并且安全性等同于其中最弱的系统。使用防火墙可以带来如下好处。

（1）防火墙允许网络管理员定义一个中心扼制点来防止非法用户，如黑客、网络破坏者等进入内部网络。禁止存在安全脆弱性的服务进出网络，并抗击来自各种路线的攻击。

（2）在防火墙上可以很方便地监视网络的安全性，并产生警报。

（3）过去的几年里，Internet 经历了地址空间的危机，使得 IP 地址越来越少。这意味着想进入 Internet 的机构可能申请不到足够的 IP 地址来满足其内部网络上用户的需要。防火墙可以作为部署网络地址变换（network address translator，NAT）的逻辑地址。因此防火墙可以用来缓解地址空间短缺的问题并消除机构在变换 ISP 时带来的重新编址的麻烦。

（4）防火墙是审计和记录 Internet 使用量的一个最佳地方。网络管理员可以在此向管理部门提供 Internet 连接的费用情况，查出潜在的带宽瓶颈的位置，并能够根据机构的核算模式提供部门级的记费。

（5）防火墙也可以成为向客户发布信息的地点。Internet 防火墙作为部署 WWW 服务器和 FTP 服务器的地点非常理想，还可以对防火墙进行配置，允许 Internet 访问上述服务，而禁止外部对受保护的内部网络上其他系统的访问。

**4. 防火墙的局限性**

防火墙无法防范通过防火墙以外的其他途径的攻击。例如在一个被保护的网络上有一个没有限制的拨出存在，内部网络上的用户就可以直接通过 SLIP 或 PPP 连接进入 Internet，如图 7-2 所示。这就为从后门攻击创造了极大的可能，网络上的用户们必须了解这种类型的连接对于一个有全面的安全保护系统来说是绝对不允许的。

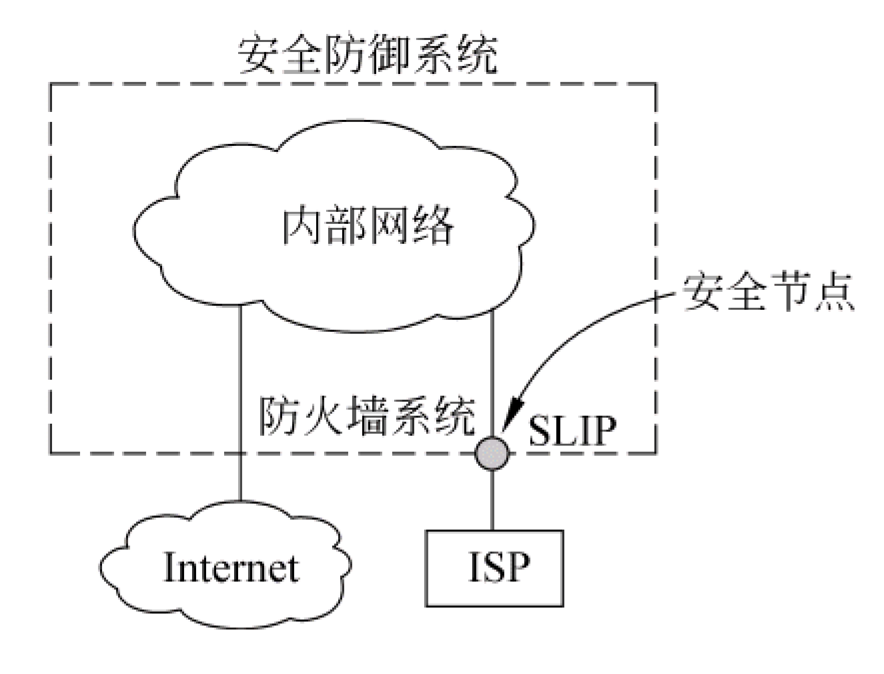



**图 7-2 绕过防火墙系统的连接**

防火墙也不能防止来自内部用户们带来的威胁。防火墙无法禁止内部用户敏感数据复制到软盘上，并将其带出公司。防火墙也不能防范伪装成超级用户或诈称新雇员，从而劝说没有防范心理的用户公开密码或授予其临时的网络访问权限。所以，必须对用户进行教育，让他们了解网络攻击的各种类型，并懂得保护自己的用户密码和周期性变换密码的必要性。

防火墙也不能防止传送已感染病毒的软件或文件，因为病毒的类型太多，操作系统也有多种，编码与压缩二进制文件的方法也各不相同，所以不能期望防火墙去对每一个文件进行扫描，查出潜在的病毒。对病毒特别关心的机构应在每个 PC 部署防病毒软件，防止病毒从软盘或其他来源进入网络系统。

最后一点是，防火墙无法防范数据驱动型的攻击。数据驱动型的攻击从表面上看是无害的数据被邮寄或复制到主机上，一旦执行就开始攻击。例如一个数据型攻击可能导

致主机修改与安全相关的文件，使得入侵者很容易获得对系统的访问权。在堡垒主机上部署代理服务器是禁止从外部直接产生网络连接的最佳方式，并能减少数据驱动型攻击的威胁。

## 7.1.2 防火墙的类型

尽管防火墙的发展已有 20 多年，但按照防火墙对内外来往数据的处理方法，大致可以分为包过滤防火墙和代理防火墙 2 大体系。

### 1. 网络级防火墙

网络级防火墙也称为包过滤防火墙，一般是基于源地址和目的地址、应用协议以及每个 IP 包的端口来作出通过与否的判断。一个路由器便是一个“传统”的网络级防火墙，它通过检查这些信息来决定是否将所收到的包转发，但它不能判断这个 IP 包来自何方，去向何方。

网络级防火墙可以判断这一点，它可以提供内部信息以说明所通过的连接状态和一些数据流的内容，把判断的信息同规则表进行比较，包过滤规则一般存放于路由器的 ACL 中。在 ACL 中定义了各种规则来表明是否同意或拒绝数据包的通过。包过滤防火墙检查数据流中每个数据包的报头信息并与过滤规则进行匹配，如果规则允许此数据包通过，该数据包就会按照路由表中的信息被转发，如果规则拒绝该数据包通过，那么该数据包就会被丢弃，ACL 对数据包的过滤如图 7-3 所示。如果没有一条规则能匹配，防火墙就会使用默认规则。一般情况下，默认规则要求防火墙丢弃该包。包过滤的核心是安全策略即包过滤算法的设计，图 7-4 解释了 ACL 处理入数据包的过程。其次，通过定义基于 TCP 或 UDP 数据包的端口号，防火墙能够判断是否允许建立特定的连接，如 TCP、FTP 连接。

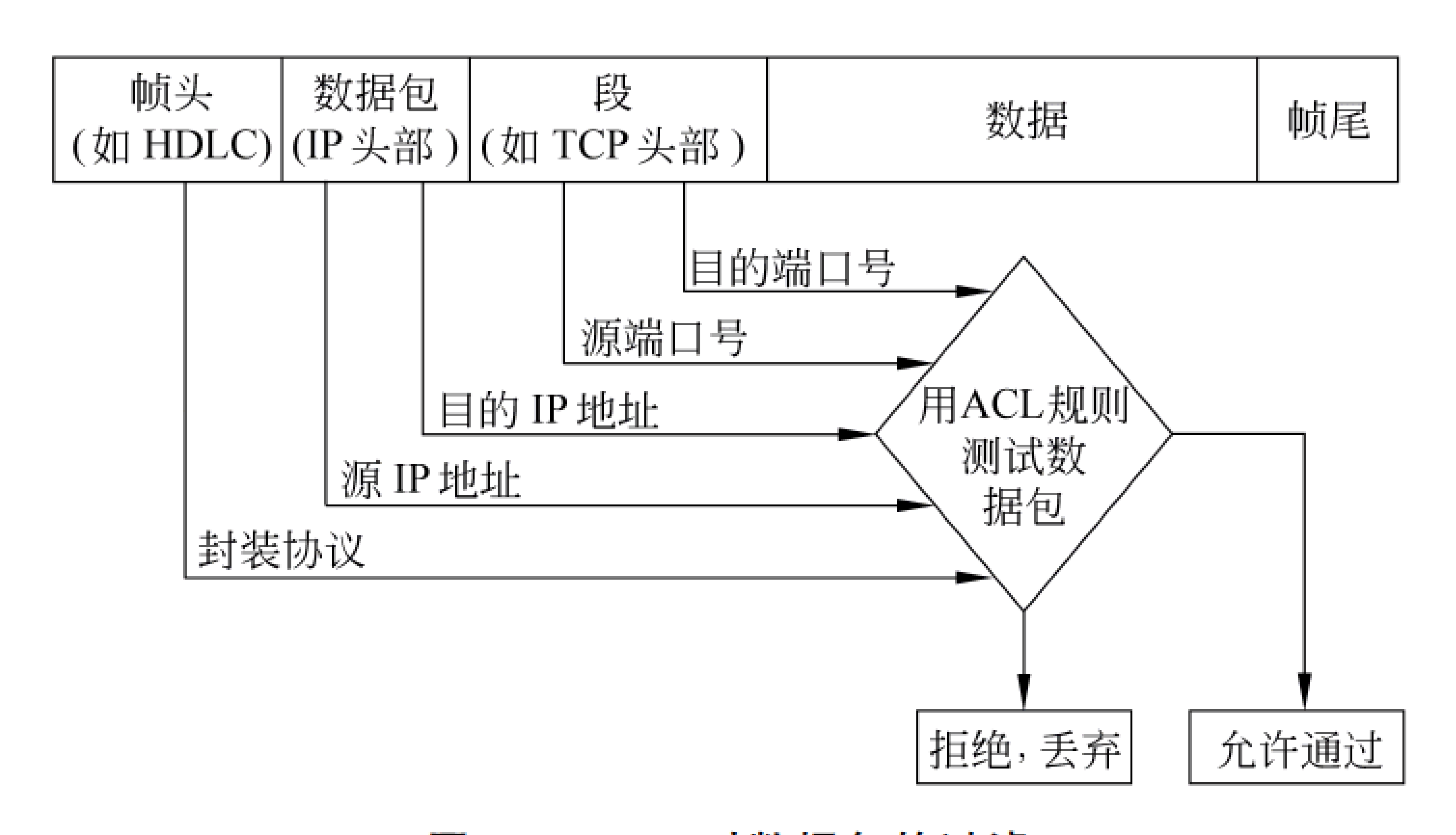



**图 7-3　ACL 对数据包的过滤**

包过滤防火墙系统只在网络层检查数据包，与应用层无关。这样系统就具有很好的传输性能，可扩展能力强。但作为系统对应用层信息无感知，无法识别通信的内容，可能被黑客所攻破，因此，包过滤防火墙的安全性有一定的缺陷。

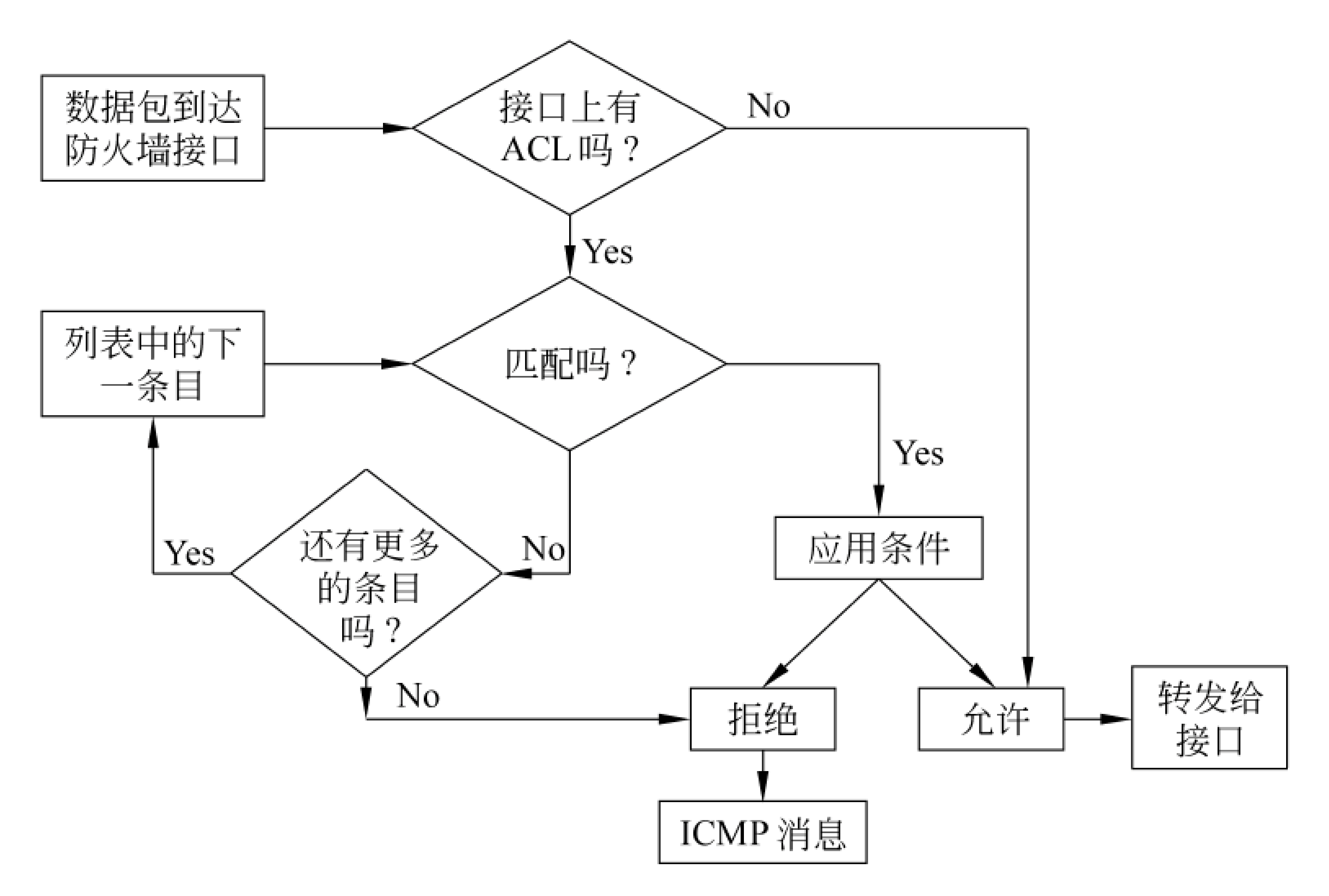



图 7-4 ACL 对入数据包的处理过程

## 2. 代理服务器防火墙

代理服务器(proxy server)防火墙是基于软件的。运行在内部用户和外部主机之间，并且在它们之间转发数据，它像真的墙一样挡在内部网和 Internet 之间。从外面来的访问者只能看到代理服务器但看不见任何内部资源；而内部客户根本感觉不到代理服务器的存在，他们可以自由访问外部站点。代理服务器可以提供极好的访问控制、登录能力以及地址转换功能，对进出防火墙的信息进行记录，便于管理员监视和管理系统，可以实现比包过滤更严格的安全策略。

下面是主机 A 试图访问 www.sohu.com，信息通过代理服务器到达网关，主机 A 发出连接请求的工作过程如图 7-5 所示。

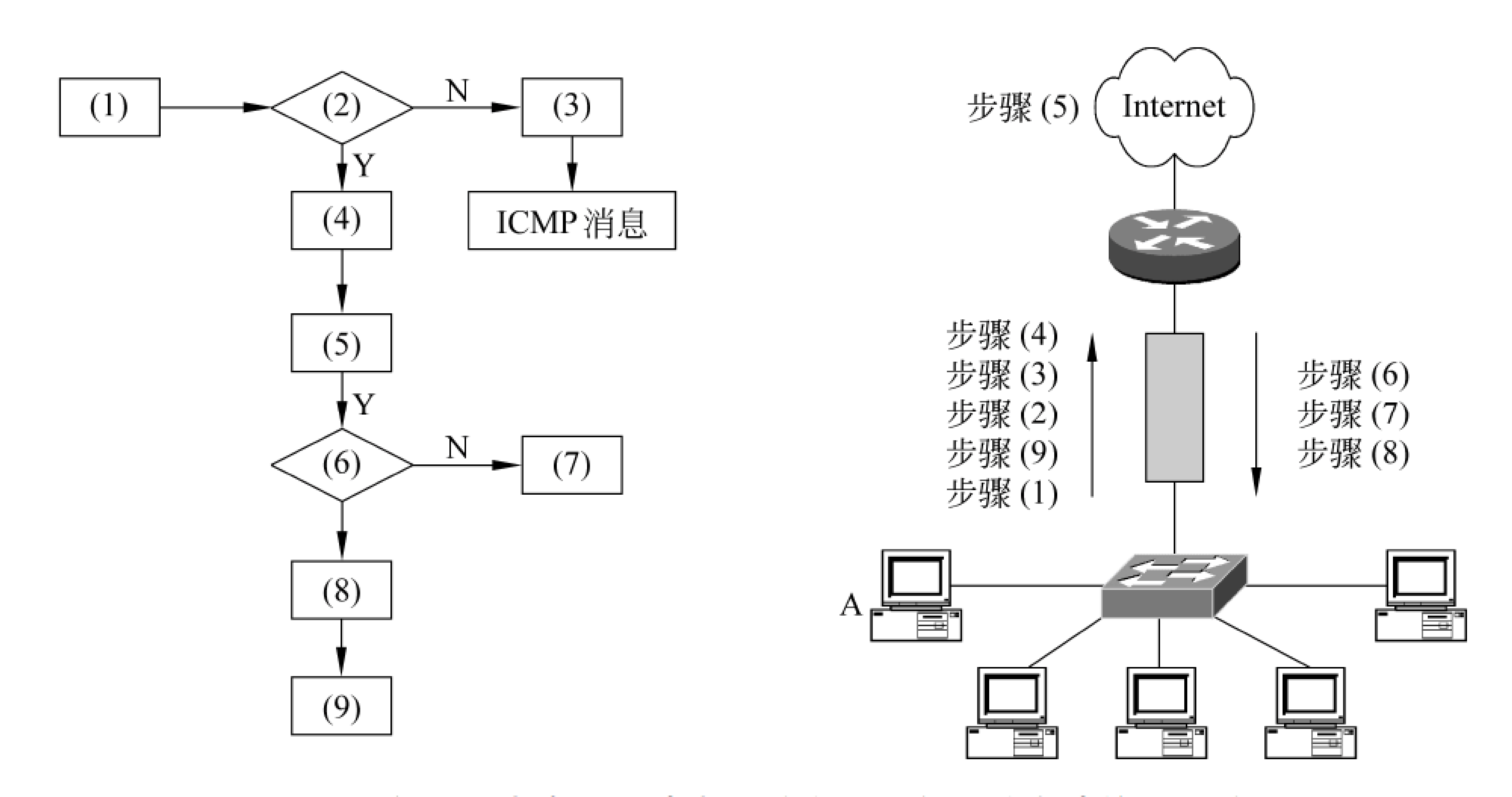



图 7-5 主机 A 发出连接请求通过代理服务器防火墙的处理过程

（1）主机 A 发出访问 Web 站点的请求。

（2）请求到达代理服务器，代理服务器检查防火墙规则集，检查数据包报头信息和数据。

（3）如果不允许该请求发出，代理服务器拒绝该请求，发送 ICMP 消息给主机 A。

（4）如果允许该请求发出，代理服务器修改源 IP 地址，创建数据包。

（5）代理服务器将数据包发给目的计算机，数据包显示源 IP 地址来自代理服务器。

（6）返回的数据包又被发送到代理服务器。服务器再次根据防火墙规则集检查数据包报头信息和数据。

（7）如果不允许该数据包进入内部网，代理服务器丢弃该数据包。

（8）如果允许该数据包进入内部网，代理服务器将它发给最先发出请求的计算机。

（9）数据包到达主机 A，此时数据包显示来自外部主机而不是代理服务器。

通过对代理服务器和包过滤器进行比较，可以了解它们提供的网络安全有什么不同。

（1）代理服务器对整个 IP 包的数据进行扫描，因此它提供比包过滤器更详细的日志文件。

（2）如果数据包和包过滤规则匹配，就允许数据包通过防火墙，而代理服务器要用新的源 IP 地址重建数据包，这样对外隐藏了内部用户。

（3）使用代理服务器，意味着在 Internet 上必须有一个服务器，且内部主机不能直接与外部主机相连。带有恶意攻击的外部数据包也就不能到达内部主机。

（4）对网络通信而言，如果包过滤器由于某种原因不能工作，可能出现的结果是所有的数据包都能到达内部网。而如果代理服务器由于某种原因不能工作，整个网络通信将被终止。

### 3. 应用网关防火墙

应用网关防火墙检查所有应用层的信息包，并将检查的内容信息放入决策过程，从而提高网络的安全性，如图 7-6 所示。然而，应用网关防火墙的可伸缩性差，它是通过打破客户机/服务器模式实现的。每个客户机/服务器通信需要两个连接：一个是从客户端到防火墙，另一个是从防火墙到服务器。还有，每个代理需要一个不同的应用进程，或一个后台运行的服务程序。对每个新的应用必须添加针对此应用的服务程序，否则不能使用该服务。

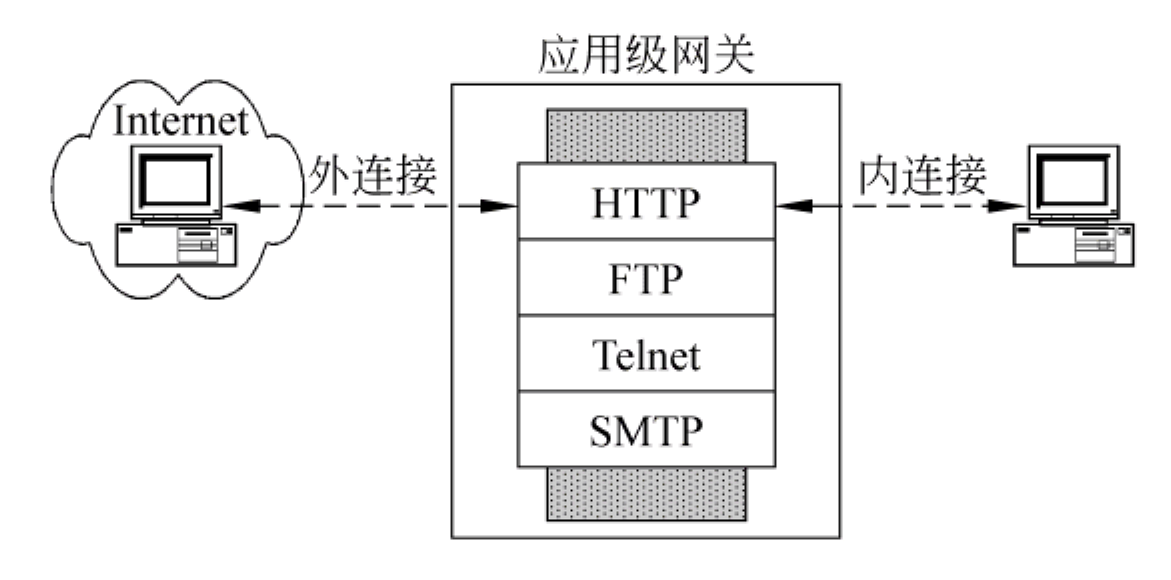



**图 7-6 应用级网关防火墙示意图**

常用的应用级防火墙已有了相应的代理服务器，例如HTTP、NNTP、FTP、Telnet、rlogin、X-Window等。但是，对于新开发的应用，尚没有相应的代理服务，它们将通过网络级防火墙和一般的代理服务。

应用级网关有较好的访问控制，是目前最安全的防火墙技术，但实现困难，而且有的应用级网关缺乏"透明度"。在实际使用中，用户在受信任的网络上通过防火墙访问Internet时，经常会发现存在延迟并且必须进行多次登录(Login)才能访问Internet或Intranet。

例如一个Telnet服务器允许远程管理员对其执行某些特定的操作。该Telnet网关对Internet可见，但是隐藏了其真实主机名，以便不受信任的网络不能识别它的真实身份，连接它的过程如图7-7所示。

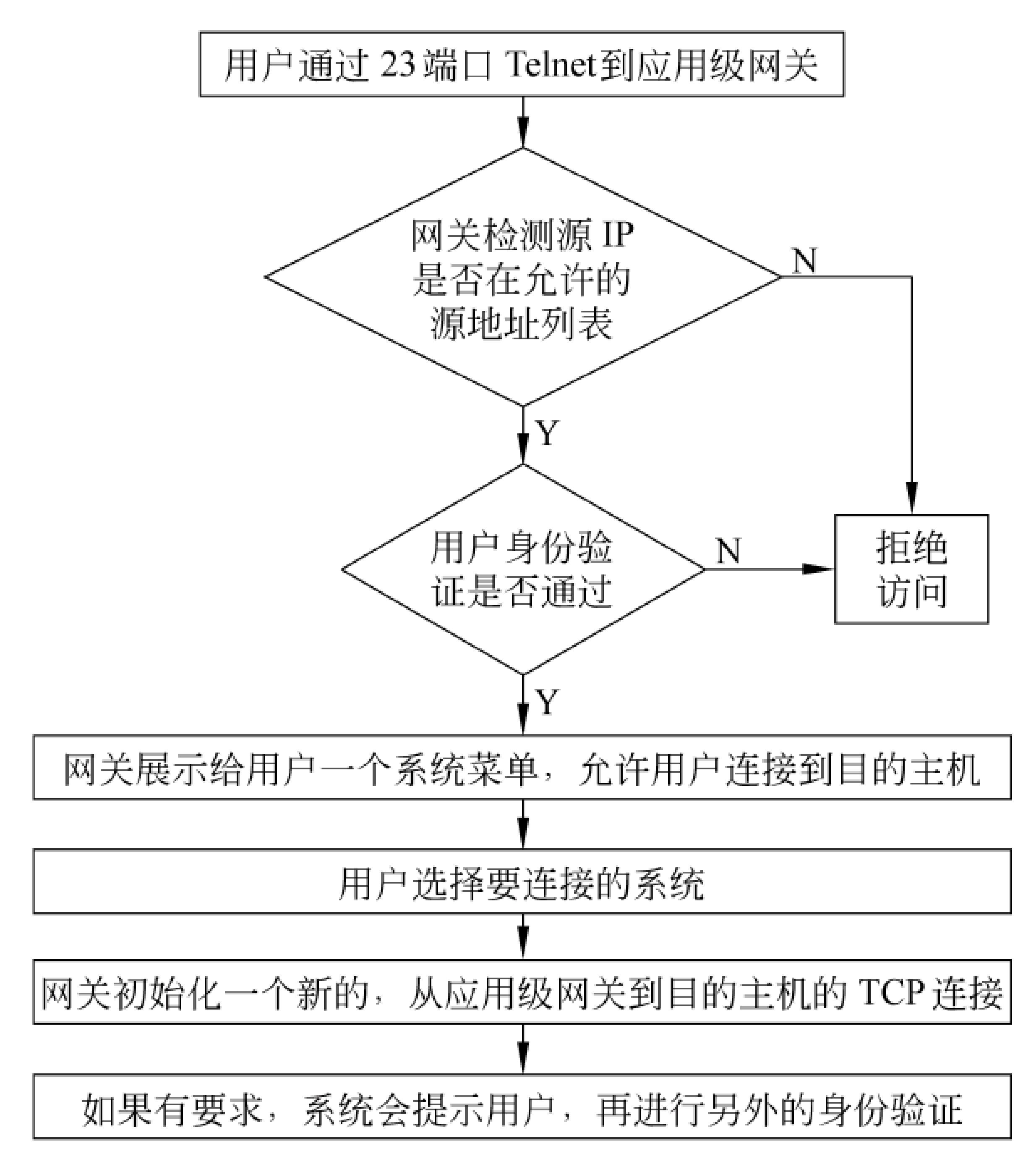



图7-7　远程连接应用网关防火墙过程

应用级网关一般由双宿主主机或者多宿主主机(在主机至少插有两块网卡)担任。在本例中，应用级网关有两块网卡，一块用于连接受保护的内部网，一块连接Internet。应用级网关的优点是能够有效地实现防火墙内外计算机系统的隔离，还可用于实施较强的数据流监控、过滤、记录和报告等功能。缺点是实现麻烦，对于那些为了使用代理服务器而修改自己应用的终端用户来说，这种选择缺乏透明度。另外由于代理服务器必须采用操作系统服务来执行代理过程，所以它通常是建立在操作系统之上的，由此带来的问题是增加了开销、降低了性能，而且由于通用操作系统是众所周知的，该操作系统的漏洞也是公开的，容易被攻击。

#### 4. 电路级防火墙

电路级防火墙用来监控受信任的客户或服务器与不受信任的主机间的 TCP 握手信息，这样来决定该会话(session)是否合法。电路级防火墙是在 OSI 模型中会话层上来过滤数据包，这样比包过滤防火墙要高二层。

电路级网关通过在 TCP 三次握手建立连接的过程中，检查双方的 SYN、ASK 和序列号是否合乎逻辑，来判断该请求的会话是否合法。一旦网关认为会话是合法的，就为双方建立连接并维护一张合法会话连接表，当会话信息与表中的条目匹配时才允许数据通过。会话结束后，表中的条目就被删除。

电路级网关与包过滤防火墙都是依靠特定的逻辑来判断是否允许数据包通过，然而包过滤防火墙允许内、外网的计算机直接建立连接，电路级网关则不允许 TCP 端到端的连接，而是要建立两个连接，其中一个连接是网关到内部主机，另一个是网关到外部主机。一旦两个连接被建立，网关只简单地进行数据中转，即它只在内部连接和外部连接之间来回复制字节并将源 IP 地址转换为自己的地址，使外界认为是网关和目的地址在进行连接。电路级网关防火墙如图 7-8 所示。

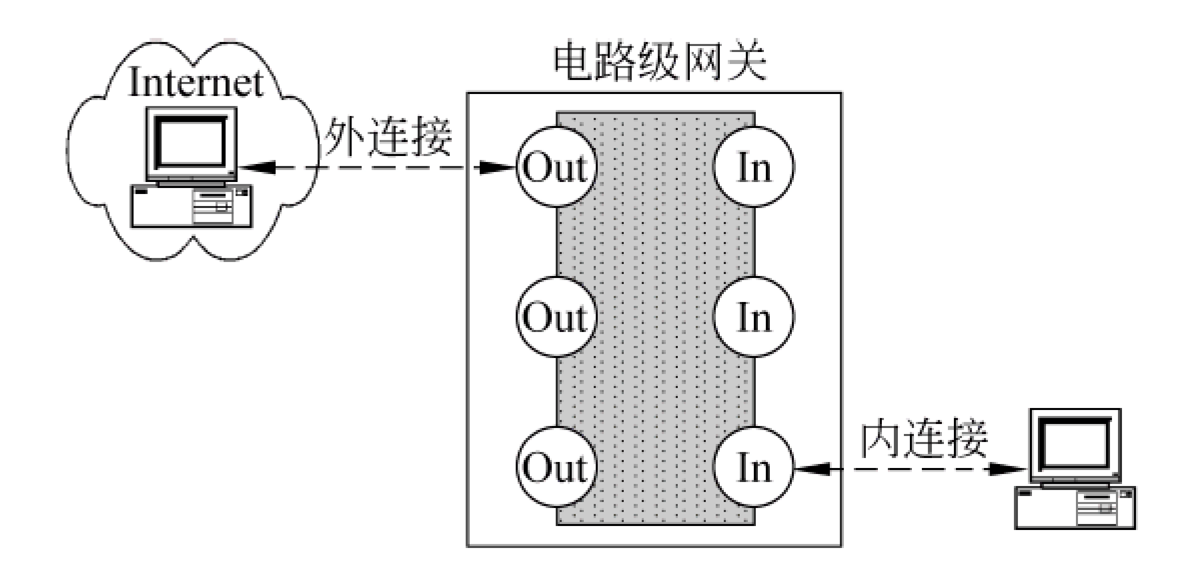



**图 7-8　电路级网关防火墙示意图**

实际上电路级防火墙并非作为一个独立的产品存在，它与其他的应用级网关结合在一起，如 Trust Information Systems 公司的 Gauntlet Internet Firewall、DEC 公司的 Alta Vista Firewall 等产品。另外，电路级防火墙还提供一个重要的安全功能，就是代理服务器(Proxy Server)。代理服务器是个防火墙，在其上运行一个叫做“地址转换”的进程，来将所有公司内部的 IP 地址映射到一个“安全”的 IP 地址，这个地址是由防火墙使用的。但是，作为电路级防火墙也存在着一些缺陷，因为该网关是在会话层工作的，它就无法检查应用层级的数据包。

例如主机 A 试图访问 www.sohu.com，它要通过一个电路级网关。下面是主机 A 发出连接请求的工作过程。

(1) 主机发出访问 Web 站点的请求。

(2) 该主机上的客户端应用程序将请求发送到电路级网关的内部接口。

(3) 如果需要身份认证，网关会提示用户进行身份认证。

(4) 如果用户的身份认证通过，网关将目的 URL 与防火墙规则集进行比较。该规则集包括允许或者禁止的 URL 列表。

(5) 如果规则集不允许进行连接，网关将拒绝访问站点的请求，并发送 ICMP 消息给

源主机。

(6) 如果规则集允许进行连接,网关向目的 URL 发出 DNS 请求,接着将自己的 IP 地址作为源 IP 地址,与目的 IP 地址建立一个连接。

(7) 网关接收到 Web 站点的应答后,将转发该应答给最先发出请求的计算机。

电路级网关实现的一个例子是 SOCKS(http://www.socks.permeo.com),包括微软的 Microsoft Proxy Server 在内的许多产品都支持 SOCKS。

电路级网关的优点是提供网络地址转换 NAT(network address translator),在使用内部网络地址机制时为网络管理员实现安全提供了很大的灵活性;基于和包过滤防火墙一样的规则具有包过滤防火墙提供的所有优点。电路级网关的缺点是电路级网关在会话建立连接后,不对所传输的内容作进一步的分析,不能很好地区分好包与坏包、易受 IP 欺骗类的攻击,需要修改应用程序和执行程序要求终端用户通过身份认证,因此安全性稍低。

### 5. 状态检测防火墙

该防火墙结合了包过滤防火墙、电路级防火墙和应用级防火墙的特点。它同包过滤防火墙一样,基本保持了简单包过滤防火墙的优点,性能比较好,能够在 OSI 网络层上通过 IP 地址和端口号,过滤进出的数据包。它也像电路级防火墙一样,能够检查 SYN 和 ACK 标记和序列数字是否逻辑有序,在防火墙的核心部分建立状态连接表,维护了连接,将进出网络的数据当成一个个的事件来处理,不仅仅考查进出网络的数据包。可以说,状态检测包过滤防火墙规范了网络层和传输层行为,大大提高了安全性。它还像应用级防火墙一样,可以在 OSI 应用层上检查数据包的内容,查看这些内容是否能符合用户网络的安全规则,其处理过程如图 7-9 所示。

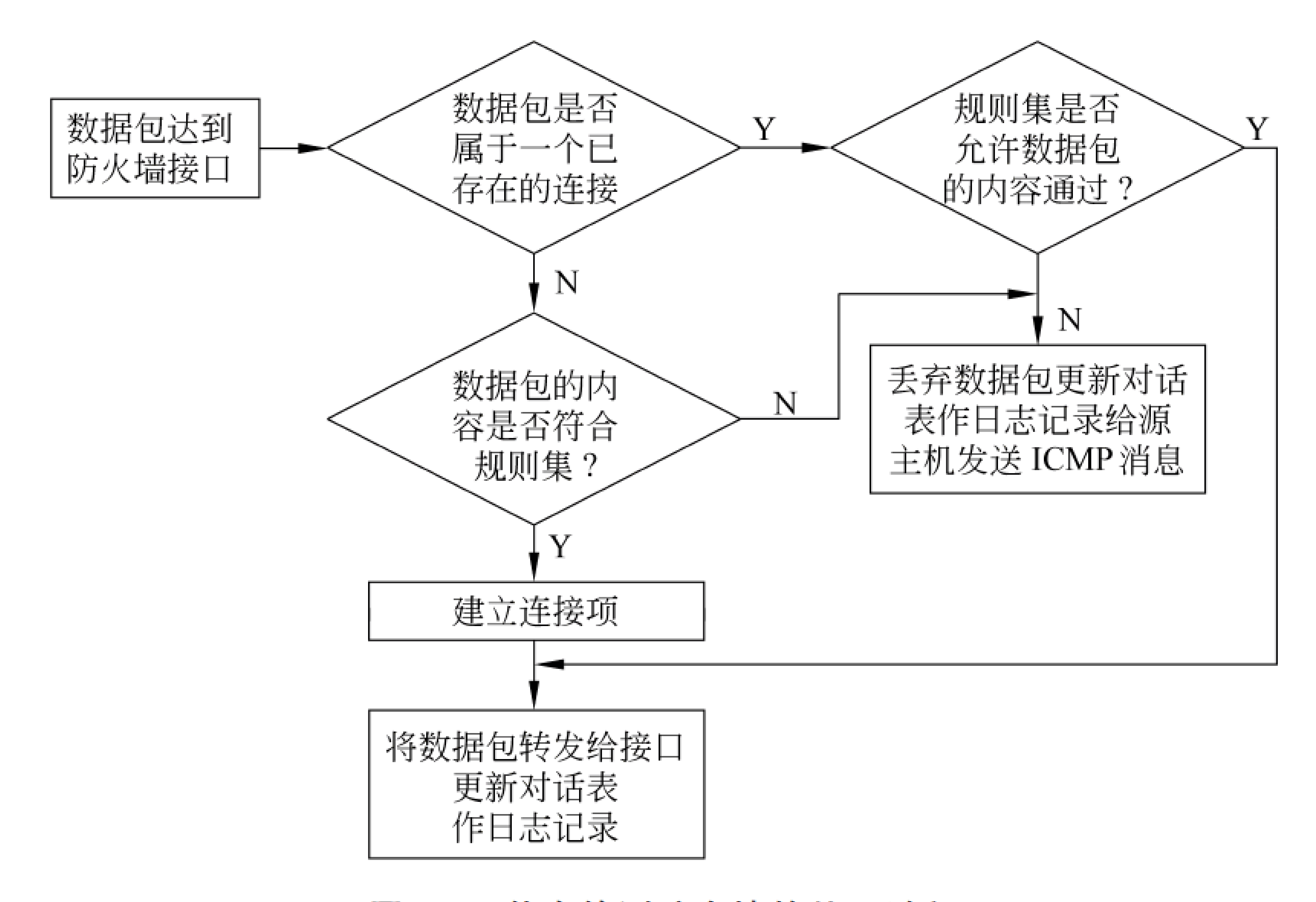



**图 7-9 状态检测防火墙的处理过程**

状态检测防火墙虽然集成前三者的特点,但是不同于应用级网关的是,它并不打破

客户/服务器模式来分析应用层的数据,它允许受信任的客户机和不受信任的主机建立直接连接。状态检测防火墙不依靠与应用层有关的代理,而是依靠某种算法来识别进出的应用层数据,这些算法通过已知合法数据包的模式来比较进出数据包,这样从理论上就能比应用级代理在过滤数据包上更有效。

下面是主机 A 试图访问 www.sohu.com 经过状态检测防火墙的例子。主机要访问 www.sohu.com,必须通过路由器,而该路由器被配置成状态检测防火墙,主机 A 发出连接请求的工作过程如图 7-10 所示。

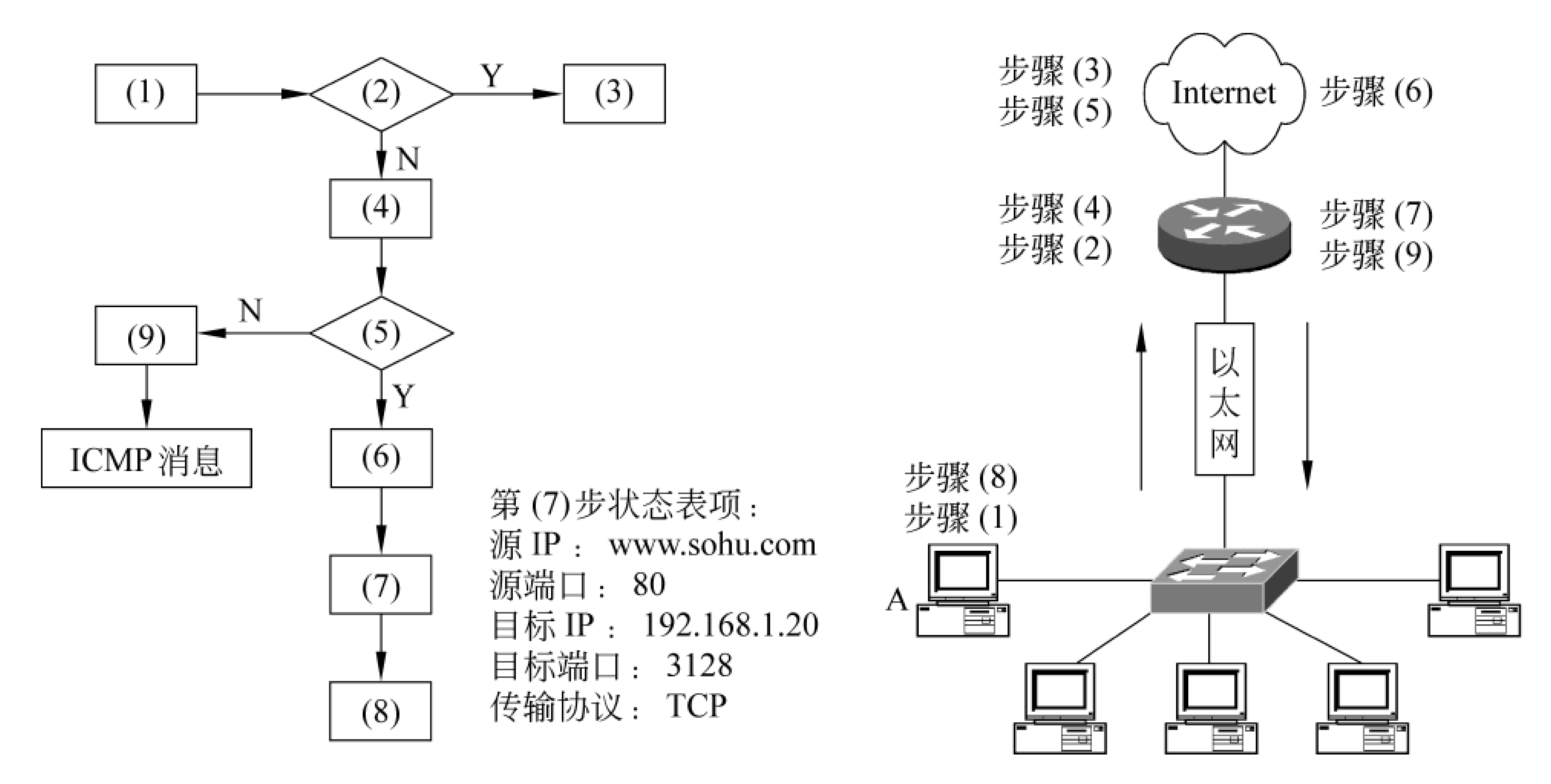



**图 7-10 主机 A 发出连接请求通过状态检测防火墙的工作过程**

(1) 主机 A 发出连接请求到 www.sohu.com。

(2) 请求到达路由器,路由器检查状态表。

(3) 如果有连接存在,且状态表正常,允许数据包通过。

(4) 如果无连接存在,创建状态项,将请求与防火墙规则集进行比较。

(5) 如果规则允许内部主机可以访问 TCP80 端口,则允许数据包通过。

(6) 数据包被 Web 服务器接收。

(7) SYN/ACK 信息回到路由器,路由器检查状态表。

(8) 状态表正确,允许数据包通过,数据包到达最先发出请求的主机 A。

(9) 如果规则不允许内部主机访问 TCP80 端口,则禁止数据包通过,路由器发送 ICMP 消息给主机 A。

与无状态包过滤相比有状态包过滤防火墙的优点是具有识别带有欺骗性源 IP 地址包的能力;检查的层面能够从网络层至应用层;具有详细记录通过的每个包的信息的能力,其中包括应用程序对包的请求、连接的持续时间、内部和外部系统所做的连接请求等。状态检测防火墙的缺点是所有这些记录、测试和分析工作可能会造成网络连接的某种迟滞,特别是在同时有许多连接激活的时候,或是有大量的过滤网络通信的规则存在时。但是硬件速度越快,这个问题就越不易察觉。

目前在市场上流行的防火墙大多属于状态检测防火墙,因为该防火墙对于用户透明,在 OSI 最高层上加密数据,不需要去修改客户端的程序,也不需对每个需要在防火墙

上运行的服务额外增加一个代理。如现在比较流行的防火墙,由 OnTechnology 软件公司生产的 OnGuard 防火墙和 CheckPoint 软件公司生产的 Firewall-1 防火墙都是一种状态检测防火墙。

### 6. 复合型防火墙

复合型防火墙是指综合了状态检测与透明代理的新一代防火墙,进一步基于 ASIC 架构,把防病毒、内容过滤整合到防火墙里,其中还包括 NAT、VPN、IDS 功能,将多单元融为一体,是一种新突破。常规的防火墙并不能防止隐蔽在网络流量里的攻击,复合型防火墙在网络界面对应用层扫描,把防病毒、内容过滤与防火墙结合起来,这体现了网络与信息安全的新思路。它在网络边界实施 OSI 第七层的内容扫描,实现了实时在网络边缘布署病毒防护、内容过滤等应用层服务措施。

1) 网络地址转换(NAT)

网络地址转换 NAT 是一种将一个 IP 地址域映射到另一个 IP 地址域的技术,从而为终端主机提供透明路由。NAT 常用于私有地址域与公用地址域的转换,以解决 IP 地址匮乏问题。在防火墙上实现 NAT 后,可以隐藏受保护网络的内部拓扑结构,在一定程度上提高网络的安全性。它可以在边界路由器、包过滤防火墙以及代理服务防火墙上实现。

2) 虚拟专用网络 VPN

虚拟专用网络(virtual private network,VPN),是在公共网络中建立专用网络,数据通过安全的加密通道在公网中传播。目前,VPN 的安全保证主要是通过防火墙技术、路由器配以隧道技术、加密协议和安全密钥来实现的,用于公司总部和分支机构、合作伙伴之间以及移动办公用户通过公网进行通信并且达到安全的目的。

3) 入侵检测系统(intrusion detection system,IDS),是主动保护自己免受攻击的一种网络安全技术。它要对侵入计算机网络和主机的行为进行发现并进行一定的阻止。通常 IDS 安装在计算机网络或计算机系统的若干关键点,进行网络和系统的信息收集和分析,从中发现网络或系统中是否有违反安全策略的行为和攻击的迹象。它扩展了系统管理员的安全管理能力(包括安全审计、监视、攻击识别和响应),提高了信息安全基础结构的完整性。

4) 认证、授权、审计

认证、授权、审计(authentication,authorization,accounting)是 Cisco 系统表述集中式身份认证服务器三大主要功能的术语,它是网络安全策略的一个组成部分。

(1) 认证

确认远端访问用户的身份,判断访问者是否为合法的网络用户,常用的办法是以一个用户标识和一个与之对应的密码来识别用户。

(2) 授权

对用户进行认证后,授权服务将决定该用户可以访问哪些资源,允许该用户执行哪些操作。

(3) 审计

为统计、计费和审计目的而记录用户使用网络服务中的所有操作,包括使用的服务

类型、起始时间、数据流量等信息。审计功能不仅保留了网络资源被使用的记录，它还可用于跟踪、记录网络访问情况并检测网络是否被入侵。

由于80%的网络攻击发生在内部，而不是外部。内部网的管理和访问控制相对外部的隔离来讲要复杂得多。对外部网的管理，基本上是禁止和放行，而对内部网管理则是针对用户来设置的。如你是谁？怎么确认你是谁？你属于什么组？该组的访问权限是什么？另外如果执行人员出现失误，网络安全也就存在问题。因此，技术越先进，审计功能就越重要。对审计的数据进行系统的挖掘，具有非常特殊的意义，通过审计也可以了解内部人员使用网络的情况或外部用户感兴趣的内容，掌握用户的兴趣和需求等。

5）服务质量

服务质量(quality of server，QoS)是网络的一种安全机制。拥有QoS的网络是一种智能网络，它可以对网络上传输的视音频流等对实时性要求较高的数据提供优先服务，从而保证较低的延迟。如果不实施QoS，IP电话电视会议及关键任务数据等应用只能作为尽力而为业务传输，这将导致在网络拥塞时话音和视频的不稳定性。

6）其他

防火墙还应包含先进的鉴别措施，如身份识别及认证、信息的保密性保护、信息的完整性校验，以及授权管理技术等。网络管理安全越完善，体系架构就越复杂。管理网络的多台安全设备，还需要集中网管。

## 7.1.3 防火墙的体系结构

要了解防火墙的体系结构，就要解释一个概念——bastion host。bastion host的中文翻译是堡垒主机，bastion是在防火墙里专门设防的地方，即设计专门用来击退进攻。网络防御的第一步，是把bastion host放置在网络中的合适位置。bastion主机为网络和Internet之间的所有通道提供一个阻塞点(choke point)。换句话说，如果不通过bastion主机，在局域网上没有计算机可以连接Internet。同样，如果不通过bastion主机，在Internet上也没有计算机可以访问局域网。如果通过一台计算机来集中网络权限，可以非常容易地掌握网络安全性。而且，通过仅使一台计算机能够访问Internet，可以更容易地配置适当的软件以保护局域网。

大多数UNIX环境，包括Linux，对维护bastion主机非常合适而且经济实惠，因为操作系统已经有能力来提供并配置防火墙。

目前，防火墙的体系结构一般有以下几种：双宿主主机体系结构；主机屏蔽体系结构；子网屏蔽体系结构。

### 1. 双宿主主机防火墙

在TCP/IP网络中，多宿主主机(multi-homed host)这个词用来描述具有多个网络接口卡的主机，如图7-11所示。通常，每个网络接口卡都和网络相连。在历史上，这种多宿主主机也可以在网络段之间传送流

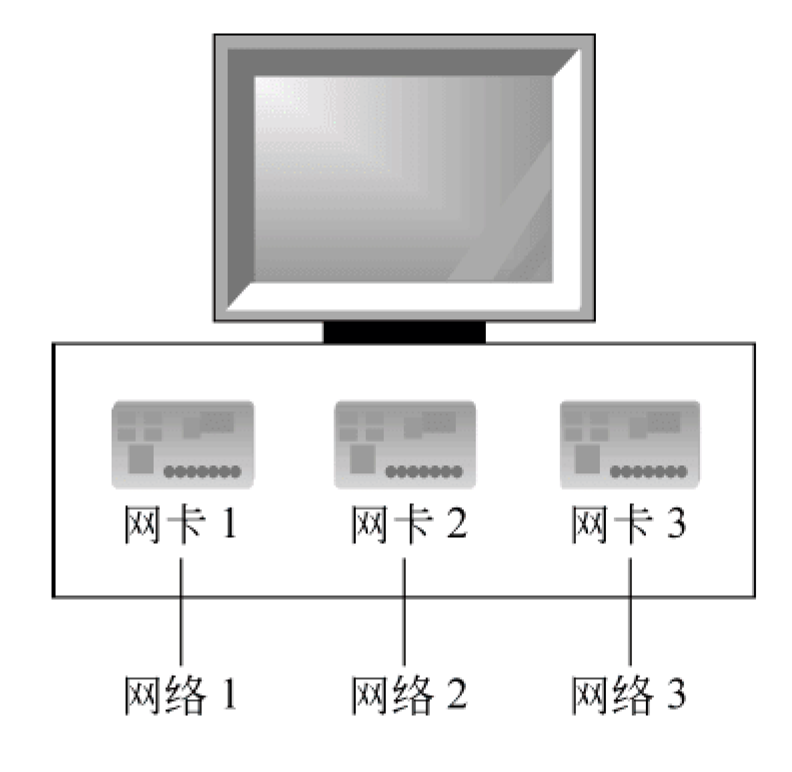


图7-11 多宿主主机防火墙

量。现在，一般都使用专门的路由器来完成IP的路由转发。

如果多宿主主机的路由功能被禁止，则主机可以在它连接的网络之间提供网络流量的分离，并且每个网络都能在宿主主机上处理应用程序。另外，如果应用程序允许，网络还可以共享数据。

双宿主主机(Dual-Homed Host)的路由功能是多宿主主机的一个特例，它有两个网络接口和被禁止的路由功能。

双宿主主机可用于把各内部网络从一个不可信的外部网络分离出来，如图7-12所示。因为双宿主主机不能转发任何TCP/IP流量，所以它可以彻底堵塞内部和外部不可信网络间的任何IP流量。

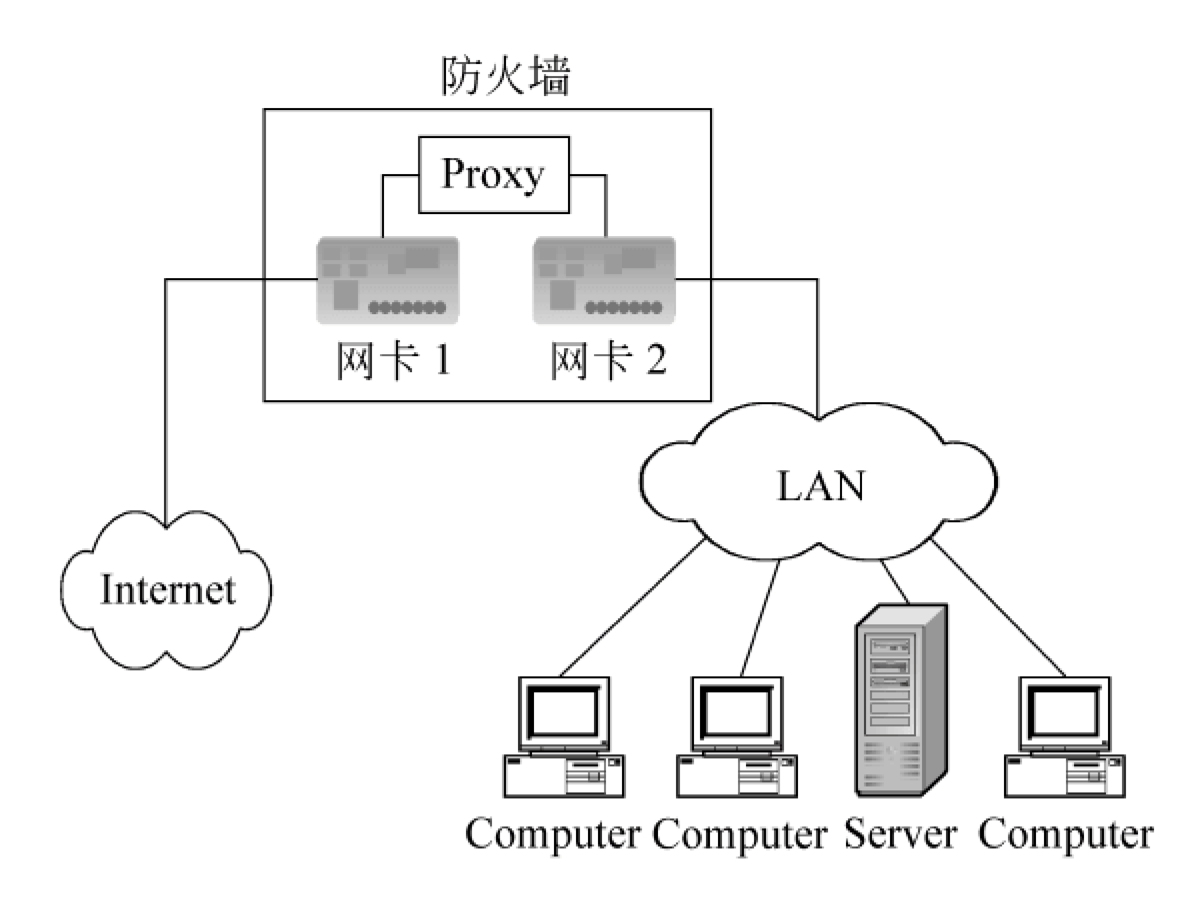



**图7-12 双宿主主机防火墙**

防火墙运行Proxy(代理)软件控制着数据包从一个网络流向另外一个网络，这样内部网络中的计算机就可以访问外部网络。双宿主主机是防火墙使用的最基本配置。建立双宿主主机防火墙的关键是要禁止路由，网络之间通信的唯一路径是通过应用层的代理软件。如果路由被意外地允许，那么双宿主主机防火墙的应用层功能就会被旁路，内部受保护网络就会完全暴露在危险之中，如图7-13所示。

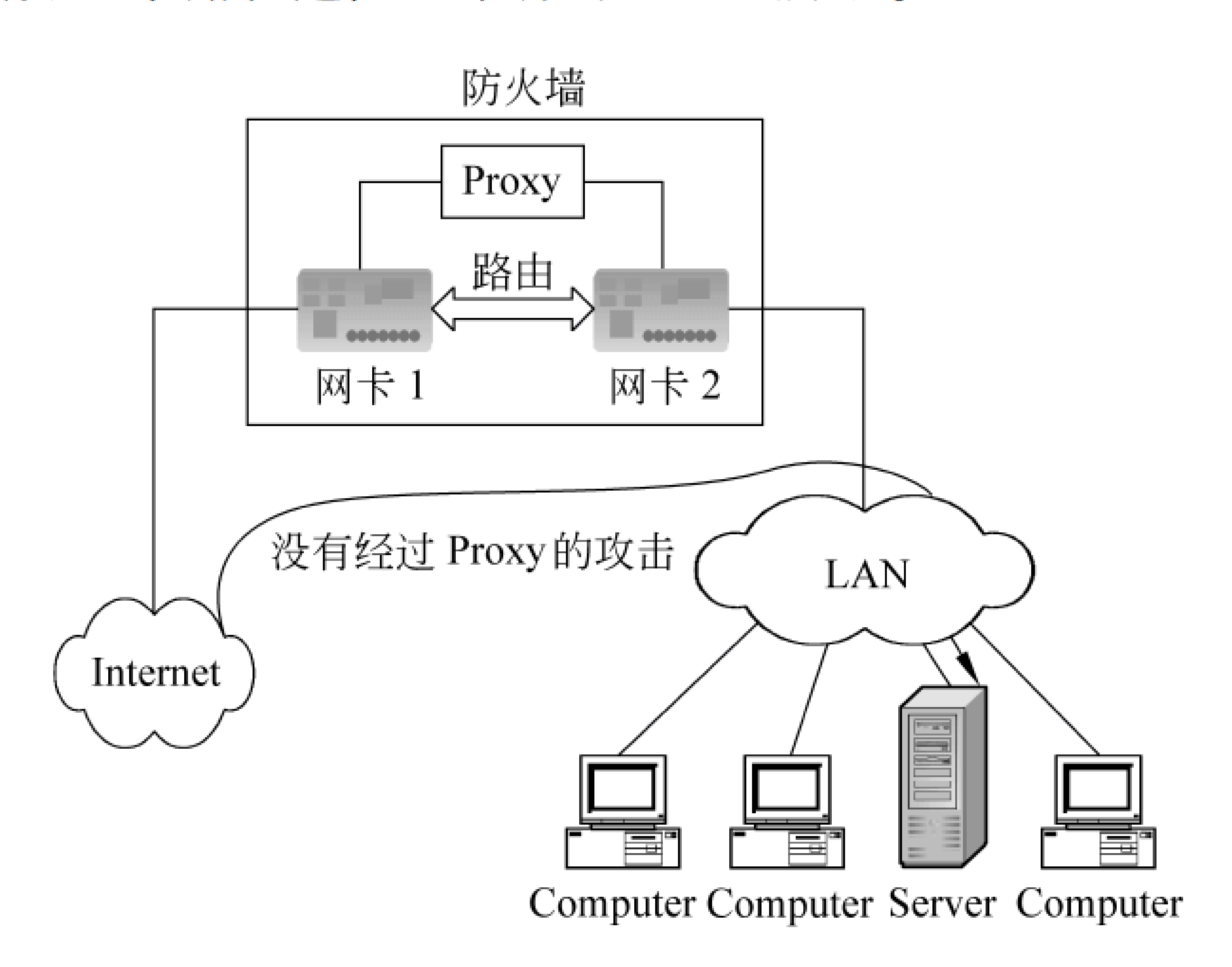



**图7-13 被旁路的双宿主主机防火墙(路由使能)**

在 UNIX 环境中运行的网络对双宿主主机防火墙的这个危险性特别敏感。在一些 UNIX 操作系统(如著名的 Berkeley UNIX)中,默认时路由能力有效。因此,在 UNIX 网络中建立防火墙时,必须认证防火墙所使用的操作系统的路由功能禁止。如果操作系统没有使路由能力失效,必须在防火墙主机内重新配置并且重建 UNIX 核心以保证操作系统使路由能力禁止。

另外,如果用户被允许直接登录到防火墙,那么防火墙的安全性就将受到危害。因为双宿主主机防火墙是内部网络和外部网络相连的中心点。一旦黑客进入到防火墙,防火墙的防卫功能也就彻底崩溃了。黑客甚至可以使用防火墙作为入侵其他主机的基地。

### 2. 主机屏蔽防火墙

一般来讲,主机屏蔽防火墙比双宿主主机防火墙更加安全。主机屏蔽防火墙体系结构在防火墙的前面增加了屏蔽路由器。也就是说,防火墙并不直接与 Internet 相连。这种配置将提供一种非常有效的并且容易维护的防火墙,如图 7-14 所示。

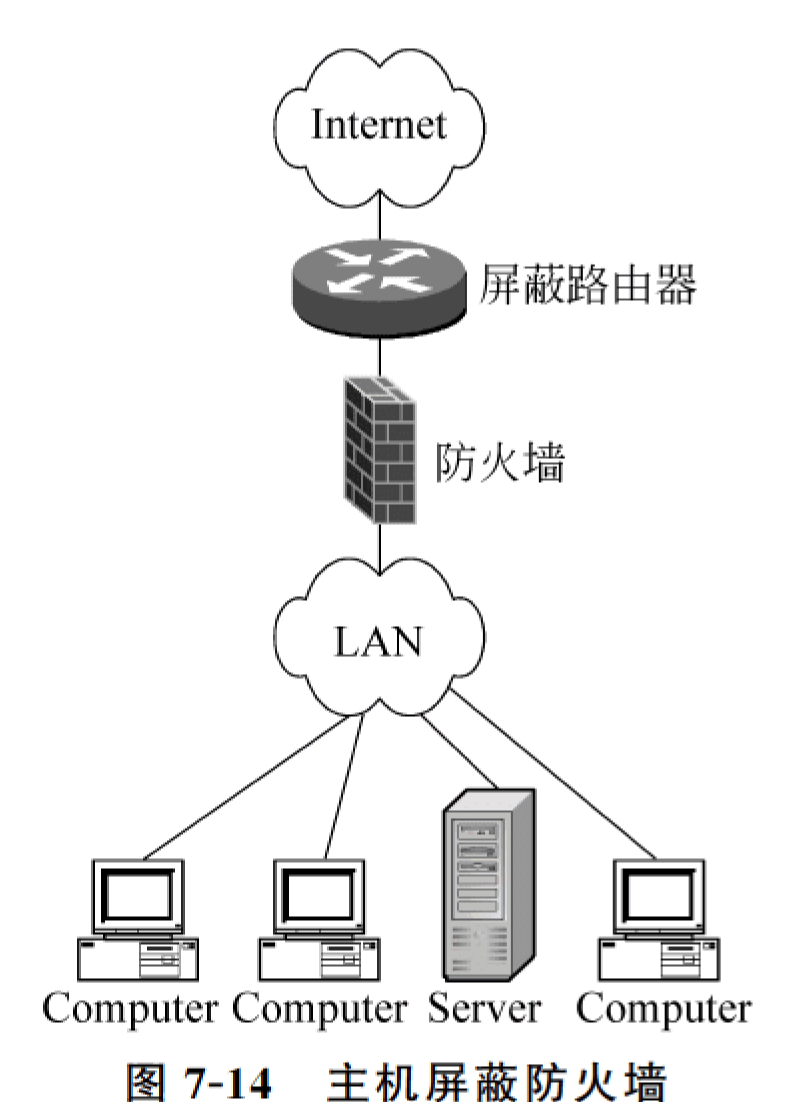


图 7-14 主机屏蔽防火墙

因为路由器具有数据过滤的功能,路由器通过适当配置(如配置访问列表)后,可以实现一部分防火墙的功能,因此有人把屏蔽路由器也称为防火墙的一种。

实际上,常常把屏蔽路由器作为从 Internet 到受保护网络的第一道防线。根据内部网络的安全策略,屏蔽路由器可以过滤掉不允许的数据包。

(1) 不允许来自内部主机(防火墙除外)的所有连接,即强迫所有内部主机必须使用防火墙代理服务。

(2) 屏蔽掉不允许的服务,如禁止 telnet、ftp、finger 请求等。

屏蔽路由器的配置要根据实际的网络安全策略,如 server 主机向 Internet 提供 www 服务,则需要在屏蔽路由器上开放对 server 主机 80 端口的访问。

因为这种体系结构允许数据包从 Internet 向内部网的移动,所以它的设计比没有外部数据包能到达内部网络的双宿主主机体系结构似乎是更具风险。话说回来,实际上双宿主主机体系结构在防备数据包从外部网络穿过内部网络时也容易产生失败(因为这种失败类型是完全出乎预料的)。进而言之,保卫路由器比保卫主机较易实现,因为它提供了非常有限的服务。多数情况下,被屏蔽的主机体系结构提供比双宿主主机体系结构更好的安全性和可用性。

### 3. 子网屏蔽防火墙

子网屏蔽体系结构添加额外的安全层到主机屏蔽体系结构,即通过添加周边网络更

进一步地把内部网络与Internet隔离开，如图 7-15 所示。

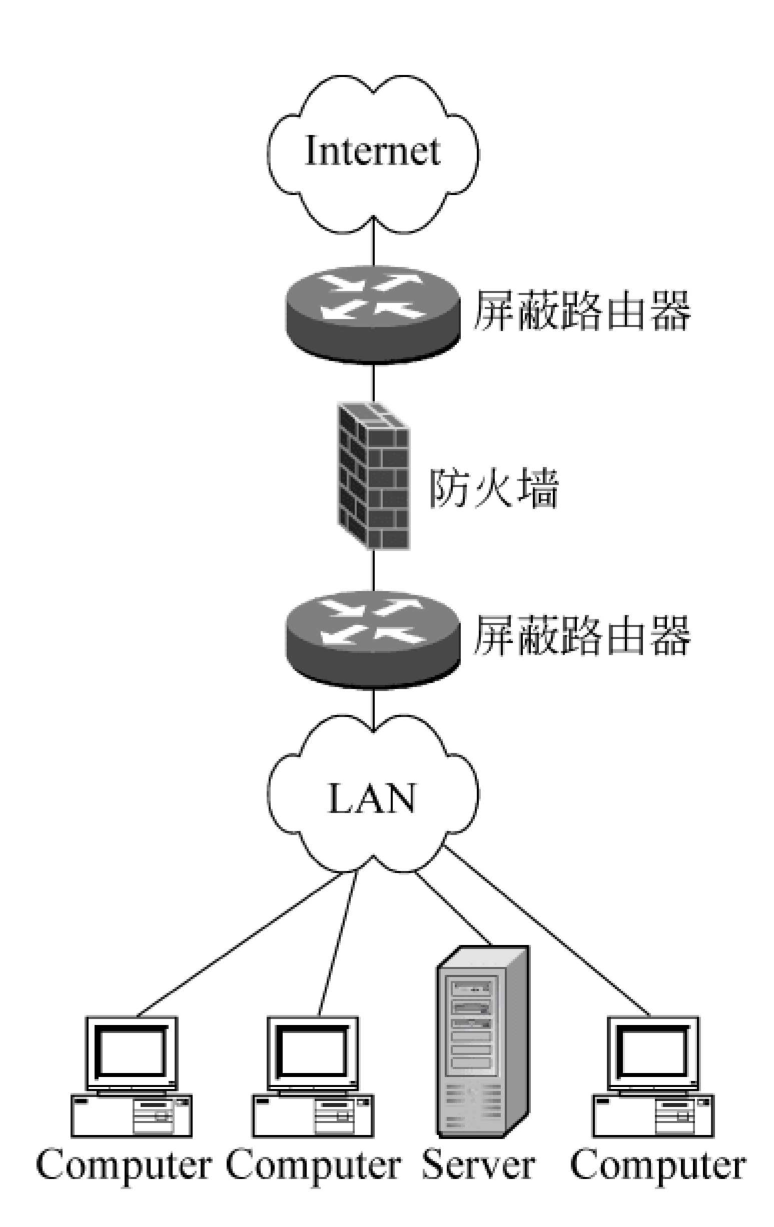



**图 7-15 子网屏蔽防火墙**

这样做是由它们的性质决定的。

堡垒主机(在这里是防火墙)是用户网络上最容易受侵袭的机器。任凭用户尽最大的力气去保护它，它仍是最有可能被侵袭的机器，没有什么主机是绝对安全的。

在主机屏蔽体系结构中，用户的内部网络对堡垒主机没有任何防御措施。如果黑客成功地侵入主机屏蔽体系结构中的堡垒主机，那就毫无阻挡地进入到内部系统。

通过在周边网络上隔离堡垒主机，能减少在堡垒主机上侵入的影响。可以说，它只给入侵者一些访问的机会，但不是全部。屏蔽子网体系结构的最简单的形式为两个屏蔽路由器，每一个都连接到周边网，一个位于周边网与内部的网络之间，另一个位于周边网与外部网络之间(通常为 Internet)。为了侵入用此类型体系结构构筑的内部网络，侵袭者必须要通过两个路由器。即使侵袭者设法侵入了堡垒主机，他仍然必须通过内部路由器。在此情况下，没有损害内部网络的单一的易受侵袭点。作为入侵者，只是进行了一次访问。

对该体系结构的要点说明如下。

1) 周边网络

周边网络是另一个安全层，是在外部网络与用户被保护的内部网络之间的附加网络。如果侵袭者成功地侵入用户防火墙的外层领域，周边网络在那个入侵者与用户的内部系统之间提供各附加的保护层。

对于周边网络的作用，举例说明如下。

在许多网络设置中，可以利用网络上的主机来侦听网络上的通信，尤其对以太网侦听更加容易(而且以太网是当今使用最广泛的局域网技术)，对若干其他成熟的技术，诸如令牌环和 FDDI 也可以侦听。入侵者可以通过侦听用户的 Telnet、FTP 以及 rlogin 会话，成功地探测出用户密码。即使密码没被攻破，探听者仍然能偷看或访问合法用户的敏感文件，或阅读他们感兴趣的电子邮件等。入侵者能完全监视何人在使用网络。

有了周边网络，如果有人侵入周边网上的堡垒主机，他仅能探听到周边网上的通信，所有的内部通信都不能越过内部的屏蔽路由器。所以，如果堡垒主机被损害，内部的通信仍将是安全的。

但是，内部网络与外部世界的通信，由于必须通过防火墙，因此仍然可以被黑客监视。要保护不在内部网络保护中的信息的完整性，最好的方式就是采用加密。

2) 堡垒主机

在子网屏蔽体系结构中，把堡垒主机连接到周边网络，这台主机便是接受来自外界连接的主要入口。例如：允许进来的电子邮件(SMTP)会话，传送电子邮件到站点；允许

进来的 FTP 连接，转接到站点的匿名 FTP 服务器；允许进来的域名服务(DNS)站点查询等。

另一方面，其出站服务(从内部的客户端到在 Internet 上的服务器)可以按如下任一方法处理。

(1) 在屏蔽路由器上设置数据包过滤来允许内部的客户端直接访问外部的服务器。

(2) 设置代理服务器在堡垒主机上运行(要求防火墙使用代理软件)来允许内部的客户端间接地访问外部的服务器。禁止内部的客户端与外部用户之间直接通信(包括拨号入网方式)。

3) 内部路由器

内部路由器(在有关防火墙著作中有时被称为阻塞路由器)保护内部的网络使之免受 Internet 和周边网络的侵犯。

内部路由器为用户的防火墙执行大部分的数据包过滤工作，它允许从内部网到 Internet 的有选择的出站服务。

内部路由器所允许的服务(堡垒主机到内部网络)和外部路由器所允许的服务(堡垒主机到 Internet)可以不同。在堡垒主机被攻破的情况下，限制堡垒主机和内部网之间服务可以减少受到堡垒主机攻击的主机的数量。

两个路由器和防火墙的具体配置要根据网络的实际安全策略决定。

4) 外部路由器

在理论上，外部路由器(在有关防火墙著作中有时被称为访问路由器)保护周边网络和内部网络使之免受来自 Internet 的侵犯，是保护内部网络的第一道防线。实际上，外部路由器倾向于允许几乎任何东西从周边网出站，并且它们通常只执行非常少的数据包过滤。保护内部机器的数据包过滤规则在内部路由器和外部路由器上基本上应该是一样的。

一般外部路由器由外部群组提供(如用户的 Internet 供应商)，同时用户对它的访问被限制。外部群组可能愿意放入一些通用型数据包过滤规则来维护路由器，但是不愿意使维护复杂或者使用频繁变化的规则组。

外部路由器能有效地执行的安全任务之一(通常别的任何地方不容易做的任务)是阻止从 Internet 上伪造源地址进来的任何数据包。这样的数据包自称来自内部的网络，但实际上是来自 Internet。

#### 4. 防火墙体系结构的组合形式

实际建造防火墙时，一般很少采用单一的技术，通常是多种解决技术的组合。这种组合主要取决于网管中心向用户提供什么样的服务，以及网管中心能接受什么样的等级风险。采用哪种技术主要取决于经费、投资的大小或技术人员的技术、时间等因素。一般有以下几种形式。

(1) 使用多堡垒主机。

(2) 合并内部路由器与外部路由器。

(3) 合并堡垒主机与外部路由器。

(4) 合并堡垒主机与内部路由器。

(5) 使用多台内部路由器。

(6) 使用多台外部路由器。

(7) 使用多个周边网络。

(8) 使用双宿主主机与屏蔽子网。

### 7.1.4 防火墙的部署

防火墙的配置是非常重要的，必须保证网络支持的协议能够通过防火墙，尤其是要让使用TCP53端口的域名系统协议(domain name system protocol)能够通过防火墙。否则的话，组织内部的机器就不能解析防火墙外的机器名字。同样，如果想让防火墙内外机器能够通信的话，也要保证防火墙外的机器能够访问相应的DNS服务器，这样它们才能解析防火墙内的主机地址。

实现防火墙的一个通常办法是拒绝绝大部分从防火墙外发起的到防火墙内机器的连接。当然特定的机器除外，这种机器是被保证严格安全的。

必须严格限制从防火墙内发起的到防火墙外的连接，必须对这种连接特别小心。必须明白谁会对网络构成威胁以及什么会构成威胁。禁止从内部发起的连接即意味着内部网连接到的主机可能就是潜在的威胁。当然如果防火墙允许任何协议通过的话，某个恶意的内部人员很容易攻破防火墙。

防火墙作为网络安全的一种防护手段，有多种实现方式。建立合理的防护系统，配置有效的防火墙应遵循如下四个基本步骤：首先进行风险分析，然后进行需求分析，接着确立安全政策，最后选择准确的防护手段并使之与安全政策保持一致。

#### 1. 包过滤路由器的配置与实现

包过滤路由器是最简单也是最常见的防火墙，它位于内部网络和外部网络之间，除具有路由功能外，可以再装上分组过滤软件，利用分组过滤规则完成基本的防火墙功能。

这种配置的优点如下。

(1) 容易实现，费用少。如果被保护网络与外界之间已经有一个独立的路由器，那么只需简单地加一个分组过滤软件便可保护整个网络。

(2) 分组过滤在网络层实现，不要求改动应用程序，也不要求用户学习任何新的东西，用户感觉不到过滤服务器的存在因而使用方便。

它的缺点如下。

(1) 没有或有很少的日志记录能力，因此网络管理员很难确定系统是否正在被入侵或已经被入侵了。

(2) 规则表随着应用的深化会很快变得很大而且复杂，这样不仅规则难以测试，而且规则结构出现漏洞的可能性也会增加。

(3) 这种防火墙的最大弱点是依靠一个单一的部件来保护系统，一旦部件出现问题会使网络的大门敞开而用户可能还不知道。

当前，几乎所有的分组过滤装置(筛选路由器或分组过滤网关)都按如下方式操作。

(1) 对于分组过滤装置的有关端口必须设置分组过滤准则,也称为分组过滤规则。

(2) 当一个分组到达过滤端口时,将对该分组的头部进行分析。大多数分组过滤装置只检查 IP、TCP 或 UDP 头部内的字段。

(3) 分组过滤规则按一定的顺序存储。当一个分组到达时,将按分组规则的存储顺序依次运用每条规则对分组进行检查。

(4) 如果一条规则阻塞传递或接收一个分组,则不允许该分组通过。

(5) 如果一条规则允许传递或接收一个分组,则允许该分组通过。

(6) 如果一个分组不满足任何规则,则该分组被阻塞。

从规则(4)和(5),可以看到将规则按适当的顺序排列是非常重要的。在配置包过滤规则时一个常犯的错误就是将包过滤规则按错误的顺序排列。如果一个包过滤规则排序有错,就有可能拒绝进行某些合法的访问,而又可能允许访问本想拒绝的服务。规则(6)遵守未被明确允许的就将被禁止的原则。

这是一个在设计安全可靠的网络时应该遵循的失效安全原则,与之相对的是一种宽容的原则,即没有被明确禁止的就是允许的。

如果采用后一种思想来设计包过滤规则,就必须仔细考虑包过滤规则没有包括的每一种可能的情况来确保网络的安全。当一个新的服务被加入到网络中时,可以很容易地遇到没有规则与之相匹配的情况。在这种情况下,可以先阻塞该服务,当听到用户因为合法的服务被阻塞而抱怨时,再允许该服务,也可以允许用户自由地访问该服务,直到制定了相应的安全规则为止。当然,这是以网络安全风险为代价的。

**2. 应用型防火墙的配置与实现**

应用型防火墙又称双宿主网关,使用双宿主主机实现。双宿主网关仅用一个代理服务器,代理服务器就是安装于双宿主主机的代理服务器软件。双宿主主机是一台有两块接口卡(NIC)的计算机,每一块接口卡有一个 IP 地址,如图 7-16 所示。如果 Internet 上的一台计算机想与 Intranet 上的一个工作站通信,它必须与双宿主主机上能“看到”的 IP 地址联系,如果规则允许的话,代理服务器软件会通过另一块网卡(NIC)启动到对方网络的连接。应该指出的是,在建立双宿主主机时,应该关闭操作系统的路由功能,否则从一块网卡(NIC)到另一块网卡的通信会绕过代理服务器软件使双宿主网关失去“防火”作用。Smart Wall 网关就是一个双宿主主机。

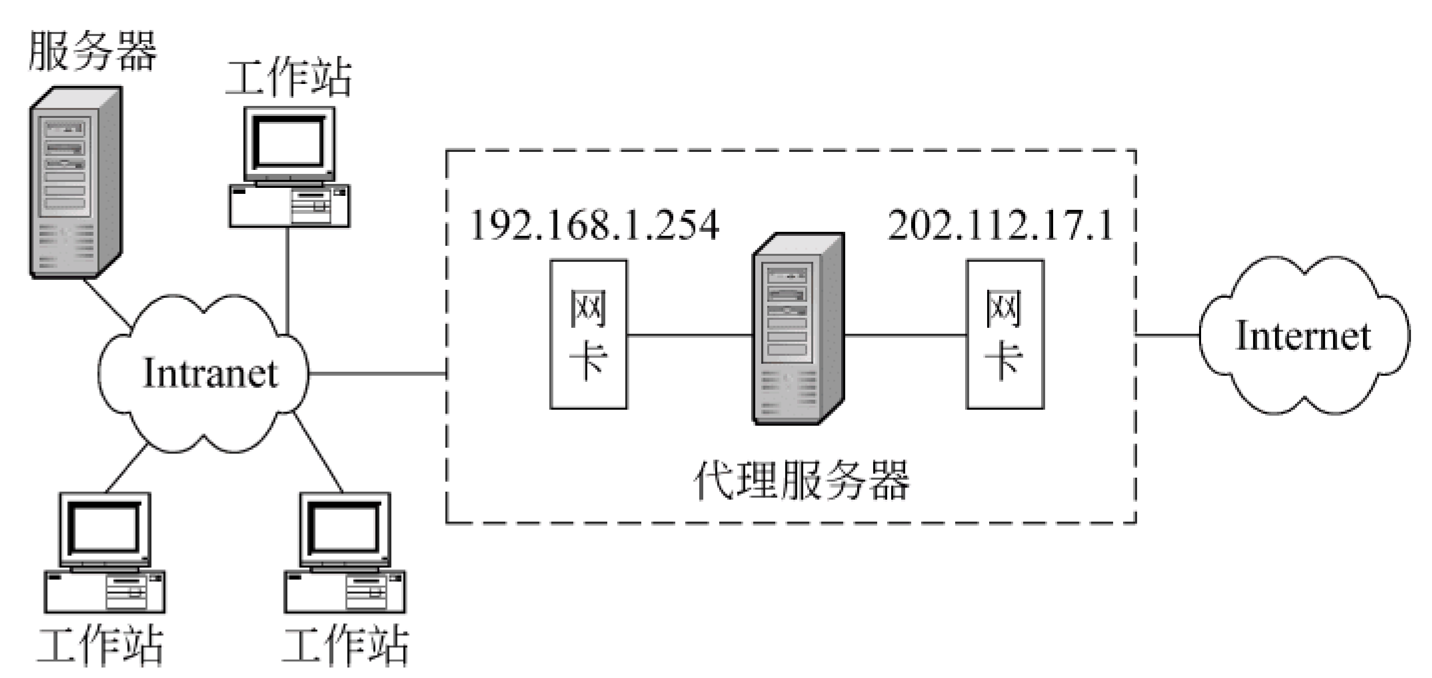



**图 7-16 应用型防火墙的配置**

双宿主网关的优点如下。

(1) 网关将受保护网络与外界完全隔离。

(2) 代理服务器提供日志,有助于发现入侵。

(3) 由于它本身是一台主机,可以用于诸如身份认证服务器及代理服务器,使其具有多种功能。

(4) 由于域名系统(DNS)的信息不会通过受保护系统传到外界,所以站点系统的名字和 IP 地址对 Internet 是隐蔽的。

双宿主网关不足之处如下。

(1) 每项服务必须使用专门设计的代理服务器,即使较新的代理服务器(如 Alta Vista Firewall)能处理几种服务,也不能同时服务。

(2) 如果防火墙只采用双宿主网关一个部件,一旦该部件出问题,将使网络安全受到危害。如果重新安装操作系统而忘记关掉路由器,将失去安全性。

### 3. 主机屏蔽防火墙的配置与实现

主机屏蔽防火墙由分组过滤路由器和应用层网关组成。在内部网络和外部网络之间建立了两道安全屏障,既实现了网络层安全(包过滤),又实现了应用层安全(代理服务)。来自 Internet 的所有通信都直接到过滤路由器,它根据所设置的规则过滤这些通信。在多数情况下与应用层网关之外机器的通信都将被拒绝。网关的代理服务器软件用自己的规则,将被允许的通信传送到受保护的网络上。在这种情况下,应用层网关只有一块网络接口卡,因此它不是双宿主网关,如图 7-17 所示。

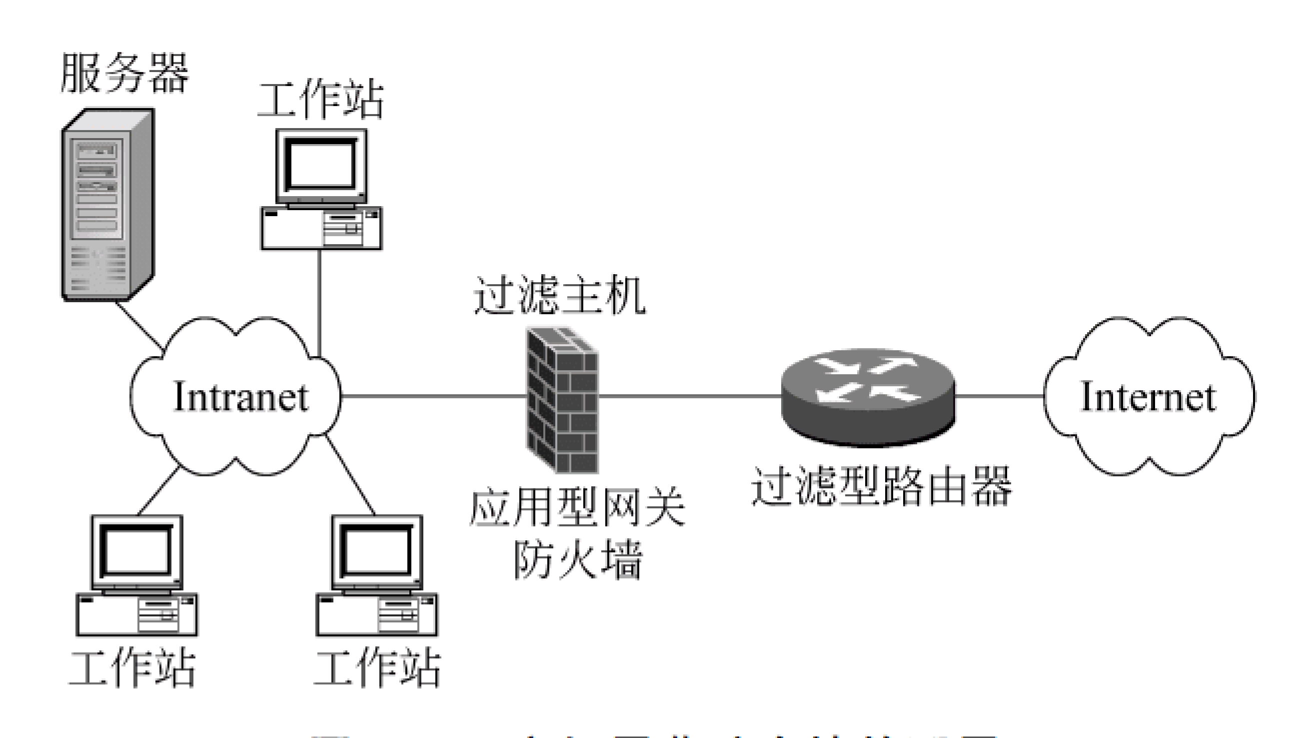



图 7-17　主机屏蔽防火墙的配置

主机屏蔽防火墙比双宿主防火墙更灵活,它可以设置成使过滤路由器将某些通信直接传到 Intranet 的站点,而不是传到应用层网关。而且包过滤路由器的规则比网络过滤简单,这是因为多数或所有通信将直接到应用层网关。此外,它具有双重保护,安全性更高。但是,要求对两个部件认真配置以便能协同工作,例如将路由器设置成使所有通信路由到代理服务器。即使包过滤规则比较简单,配置防火墙的工作也会很复杂。另外,系统的灵活性会导致走捷径而破坏安全,例如用户可能试图避开代理服务器直接与路由器建立联系。

#### 4. 子网屏蔽防火墙的配置与实现

子网屏蔽防火墙是在主机屏蔽防火墙配置上再加一个路由器，形成一个被称为非军事区的子网，这个子网还可能被用于信息服务器和其他要求严格控制的系统，从而形成三道防线，如图 7-18 所示。外部过滤路由器和应用层网关与在主机屏蔽防火墙中的功能相同。内部过滤路由器在应用层网关与受保护网络之间提供附加保护，万一入侵者通过了外部路由器和应用网关，内部路由器还可起到最后一级防御。因此，一个入侵者要进入受保护的网络比进入主机过滤防火墙更加困难。但是，它要求的设备和软件模块最多，其配置最贵且相当复杂。

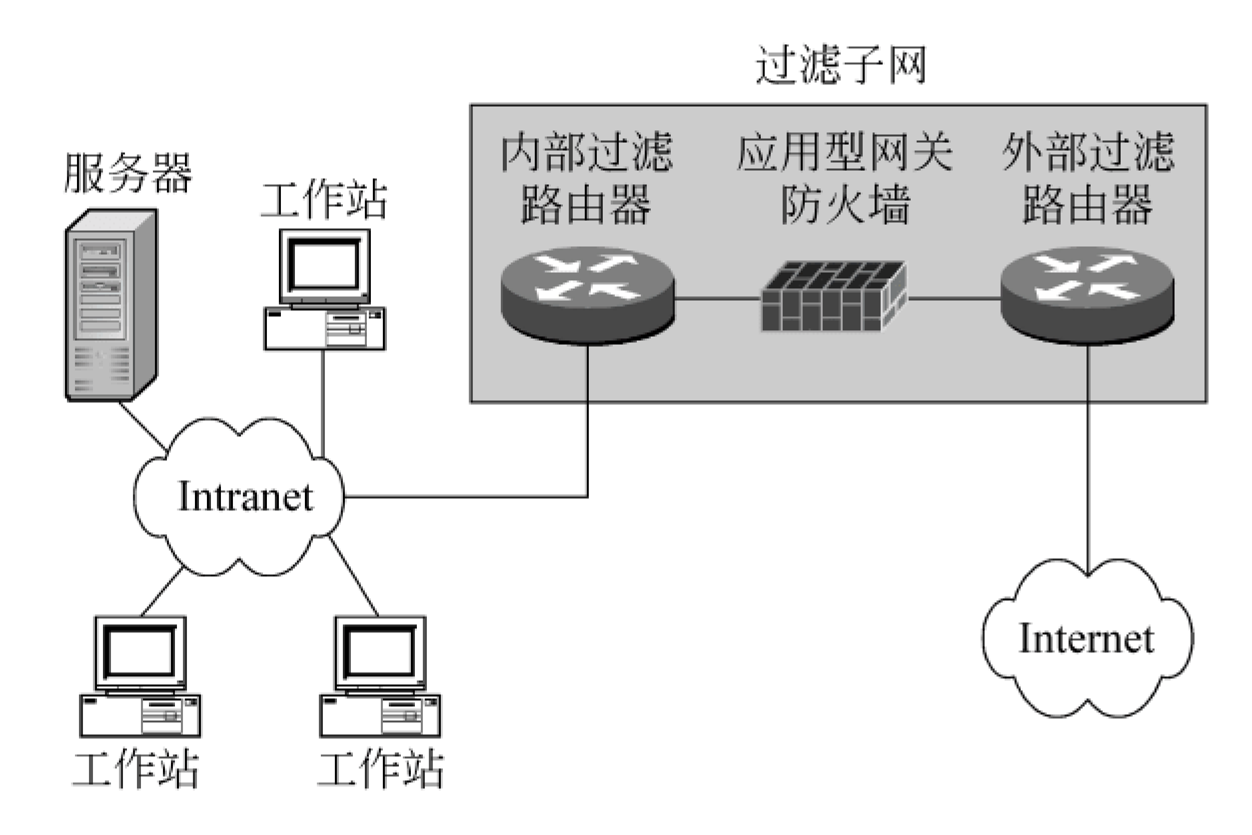



**图 7-18　子网屏蔽防火墙的配置**

#### 5. 防火墙与 Web 服务器之间的配置策略

防火墙将极大地增强内部网和 Web 站点的安全。根据不同的需要，防火墙在网中的配置有很多方式。根据防火墙和 Web 服务器所处的位置，总的可以分为三种配置：Web 服务器置于防火墙之内、Web 服务器置于防火墙之外和 Web 服务器置于防火墙之上。

1）Web 服务器置于防火墙之内

图 7-19 是防火墙作用的图示。在此模式中，Web 服务器置于防火墙之内。

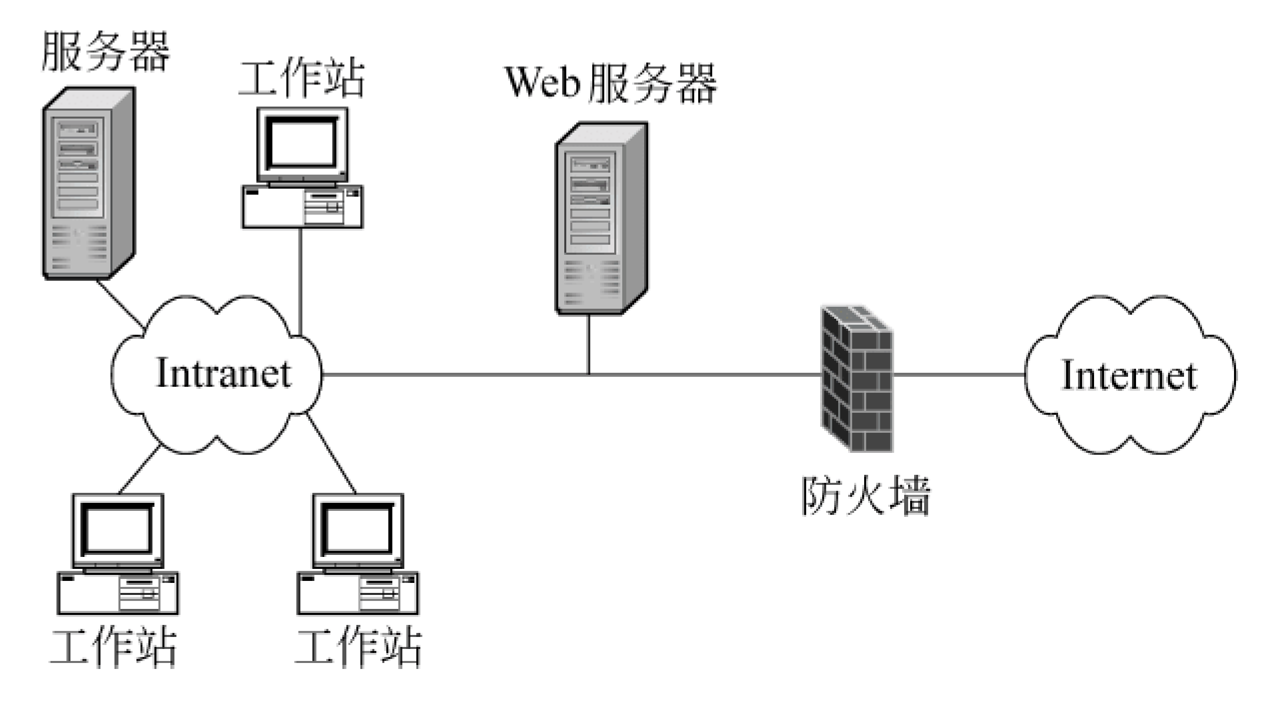



**图 7-19　Web 服务器置于防火墙之内**

将 Web 服务器装在防火墙内的好处是它得到了安全保护,不容易被黑客闯入,但不易被外界所用。当 Web 站点主要用于宣传企业形象时,显然这不是好的配置,这时应当将 Web 服务器放在防火墙之外。

2) Web 服务器置于防火墙之外

图 7-20 是 Web 服务器置于防火墙之外的配置图示。

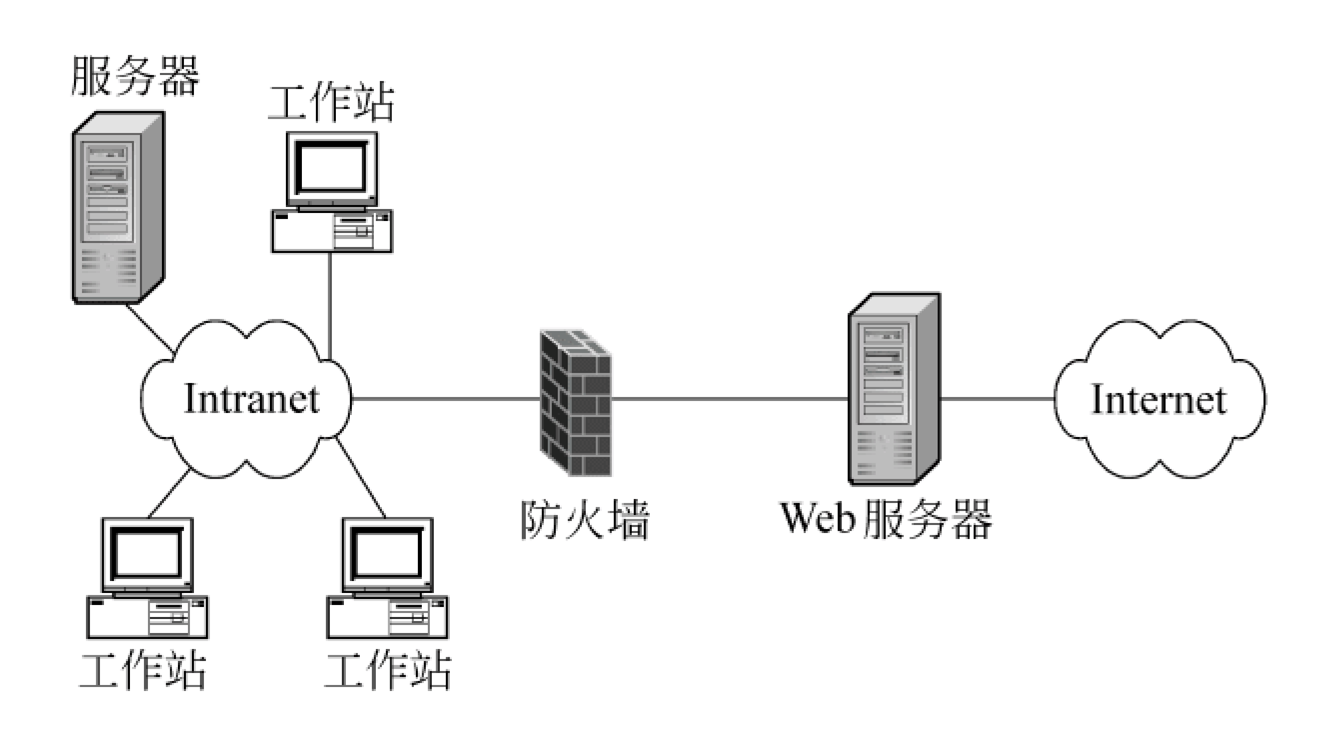



**图 7-20 Web 服务器置于防火墙之外**

事实上,为保证内部网络的安全将 Web 服务器完全置于防火墙之外是比较合适的。在这种模式中,Web 服务器不受保护,但内部网则处于保护之下,即使黑客闯进了受保护的 Web 站点,内部网络仍是安全的。代理支持在此十分重要,特别是在这种配置中,防火墙对 Web 站点的保护几乎不起作用。

3) Web 服务器置于防火墙之上

一些管理者试图在防火墙机器上运行 Web 服务器,以此增强 Web 站点的安全性。这种配置的缺点是一旦服务器有一点毛病,整个组织和 Web 站点就全部处于危险之中。图 7-21 是此种配置的图示。

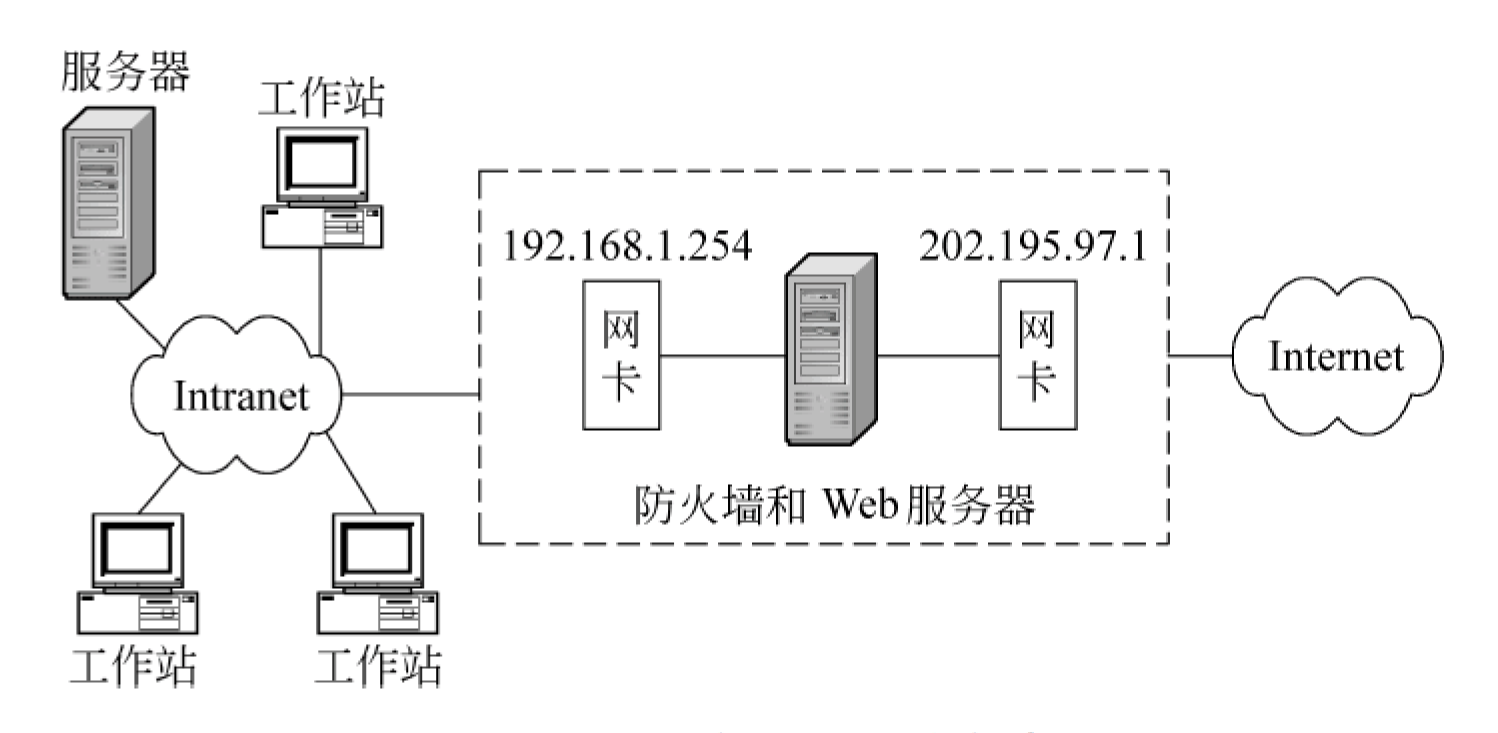



**图 7-21 Web 服务器置于防火墙之上**

这种基本配置有多种变化,包括利用代理服务器、双重防火墙、利用成对的“入”、“出”服务器提供对公众信息的访问及内部网络对私人文档的访问。

一些防火墙的结构不允许将 Web 服务器设置其外。在这种情况下将不得不打通防火墙,具体步骤如下。

(1) 允许防火墙传递对端口 80 的请求,访问请求或被限制到 Web 站点或从 Web 站

点返回(假定正使用“主机屏蔽型”防火墙)。

(2) 可在防火墙机器上安装代理服务器,但需要一个“双宿主网关”类型的防火墙。来自 Web 服务器的所有访问请求在被代理服务器截获之后才传给服务器。对访问请求的回答直接返回给请求者。

### 7.1.5 防火墙的选择因素

防火墙不是路由器、交换机或者服务器(虽然看起来比较像),所以不能用那些产品的指标来选择防火墙。那么选择防火墙应该注意哪些方面呢?

#### 1. 防火墙本身的安全性

这是重中之重。安全性不高的防火墙,其他性能再好也是空谈。由于防火墙本身会暴露在网络访问之下,所以其自身的安全性是一个应该优先被考虑的问题。产品本身所采用的系统架构是否健壮、是否存在安全漏洞、是否有被拒绝服务攻击击溃的历史等,功能和配置上是否可以处理 IP 欺骗、密码猜测等常见的攻击手段,这些都是衡量标准。另外还需注意的是考察防火墙所支持的认证方式,支持方式较为广泛、与网内认证措施协同较好的产品无疑具有更高的安全性。

具体来说安全性包括几个方面,自身安全性、访问控制能力和抗攻击能力。

(1) 自身安全性主要是指防火墙系统的健壮性,也就是说防火墙本身应该是难以被攻入的。还有防火墙的管理方式也很重要,如管理员采用 Telnet 还是 Web 管理防火墙,有没有加密和认证等。

(2) 访问控制能力是防火墙的核心功能。访问控制能力包括控制细度,也就是能控制哪些内容,比如地址、协议、端口、时间、用户、命令、附件等。还要注意的就是控制强度,即应该限制的内容必须全部阻断,而应该通过的内容不应该有任何阻断。

(3) 抗攻击能力是指防火墙对各种攻击的抵抗能力,包括抵御攻击的种类,数量。特别是对 DoS 和 DDoS 攻击的抵抗力。目前对于 DDoS 攻击还没有什么完善的解决办法,因此对 DDoS 攻击主要看能抵御的强度有多大。

用户在选择防火墙的时候,自己来判断以上这些性能是很困难的,因为用户没有专门的测试工具和手段。可以根据一些第三方的认证和评测来辅助判断,例如是否拥有安全性较严格的军队认证或是中国信息安全产品测评认证中心的等级证书。现在用的标准是国标 gb/t18336,一共 7 级,等级越高越好。

#### 2. 数据处理性能

防火墙是个网络设备。在保证安全的基础上,应该最大程度减少对网络数据处理性能的影响。作为选择的最重要参考项目,硬件防火墙的数据处理性能的核心主要是防火墙处理数据包的能力,如吞吐率、转发率、丢包率、缓冲能力和延迟等都是衡量硬件性能的标准。

当然,防火墙在包处理时采用的算法等因素也会在很大程度上影响防火墙在实际使用中的性能表现,这也是选购应考虑的因素。防火墙在策略起作用和全通策略的状态

下，上述指标都是不一样的，用户一定要考虑实际环境。可以先按照用户的要求添加策略（全通策略在最后）然后再测试。传说中有的百兆防火墙小包（64字节）通过率能达到70%以上，甚至90%，但实际使用中不大可能。之所以能够测试出这样的数据只有两个可能，一是采用高性能硬件，比如采用了千兆网卡芯片，二是在测试机的内核做手脚。

### 3. 网络功能

这里包括的内容就多了，有地址转换、IP/MAC绑定、静态和动态路由、源地址路由、代理、透明代理、ADSL拨号、DHCP支持、双机热备、负载均衡等。

在这些眼花缭乱的功能里，用户应该有一双明亮的眼睛。因为并不是每一个功能都需要，也不需要为了一些不需要的功能花冤枉钱。当然，价钱相等的情况下功能越多越好。应该首先明确需要什么功能，并且要确定这些功能都要达到什么效果，然后再寻找相应的设备。有些功能在不同厂家的定义是不同的，实现的效果也不一样。

### 4. 管理功能

这里面的内容也不少，不要小看了这里的东西。防火墙不像交换机，安装好了50年不用管。防火墙需要经常管理，日常的管理就是查看日志、修订策略、添加和删除用户。一款防火墙的配置管理是否容易直接决定了安全管理员的工作量，也是防火墙产品能否很好应用的重要保障。非常复杂凌乱的配置很容易造成安全策略实现上的错误，埋下安全隐患，要是在这样复杂的信息环境下，管理成本和维护成本的增加会消耗掉企业很大的开支。

更高的管理还包括第三方互动、VPN建立、远程集中管理等。在管理方面，应该注意界面的友好性，设置选项应该通俗易懂。远程管理对用户来说，要注意管理命令的加密和认证、是否支持策略远程导入导出等。至于管理的界面是否好看，那就看个人喜好了。

### 5. 日志能力

任何安全系统都有被攻破的可能，对于攻击者来说，最大的安全威胁不是部署何种安全装备，而是在攻击行为发生后，被攻击方是否有足够的证据和信息提出法律诉讼，所以在关心了功能和性能方面的参数之后，一定不要忽略防火墙产品的日志处理能力。一款日志功能强大的防火墙，日志系统应该有详细的记录，记录的项目应比较全面，包括连接的状态和内容，这样可以有效地防范日志被篡改，并能利用多种途径将日志数据定期备份到指定机器。同时，要考查防火墙产品的日志查看能力，包括查看途径的多少、信息显示的合理性等，应该便于分类和排序，应该方便存入数据库并有syslog等标准的接口。

### 6. 产品兼容性

网络安全的保障需要依赖设计良好功能完整的体系，单单靠一种产品是无法解决所有问题的，所以在选购安全产品的时候应注意该产品与其他安全部件以及现有设备之间的兼容性，否则购买之后如果在整体环境中造成冲突，将极大浪费宝贵的安全投资。像

防火墙这种通用的产品，在行业内通常都有很多开放式接口，用于产品开发者处理不同厂商和不同类型产品的互连问题。绝对没有一种产品就能全部解决问题的，很多厂商在开发不同的产品时根本就没有考虑系统互操作的问题。

**7. 质量**

防火墙的质量表现可不是做工精细不精细，而是防火墙是否能经久耐用。现在比较先进的防火墙普遍采用的是贴板技术，也就是将所有的原件都采用贴片的工艺。这样整个防火墙都是一体的，自然不容易出故障。如果防火墙的内存、网卡还采用插槽的方式，甚至还采用普通硬盘作为系统内核存储设备，那系统的稳定性就可想而知了。另外在高稳定性要求的环境里要看有没有双电源，大功率风扇等。虽然看上去是细节，但是对于防火墙的稳定运行是非常重要的。

目前，涉及防火墙产品的厂商众多，主要厂商有 Cisco、Checkpoint、NetScreen、Amaranten、Radware、熊猫、天融信、东软、联想网御、远东网安等，用户在采购前可以根据自己网络现状和网络应用向相关的厂商进行详细的咨询。总的来说，包过滤防火墙和应用网关防火墙还属于初级防火墙，对应规模不大的中型企业使用，而状态检测防火墙和复合型防火墙则拥有更强的安全性，适合大规模的企业或其他部署使用。

## 7.2 入侵检测与防御系统

网络互联以后，入侵者可以通过网络实施远程入侵。而入侵行为与正常的访问或多或少有些差别，通过收集和分析这种差别可以发现大部分的入侵行为，入侵检测技术就是应这种需求而诞生的。经入侵检测发现入侵行为后，可以采取相应的安全措施，如报警、记录、切断或拦截等，从而提高网络的安全应变能力。

### 7.2.1 入侵检测的概述

**1. 入侵检测基本概念**

入侵检测(intrusion detection)是对入侵行为的发现。它从计算机网络或计算机系统的关键点收集信息并进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。负责入侵的软硬件组合体称为入侵检测系统(IDS)。

Denning 于 1987 年提出了一种通用的入侵检测模型(IDES 原型系统)。IDES 原型系统采用的是一个混合结构，包含了一个异常检测器和一个专家系统。

图 7-22 所示为 IDES 原型系统。异常检测器采用统计技术刻画异常行为，专家系统采用基于规则的方法检测已知的危害行为。异常检测器对行为的渐变是自适应的，因此引入专家系统能有效防止逐步改变的入侵行为，提高准确率。该模型为入侵检测技术的研究提供了良好的框架结构。

入侵检测内容包括试图闯入、成功闯入、冒充其他用户、违反安全策略、合法用户的泄露、独占资源以及恶意使用等。入侵检测技术是动态安全技术的最核心技术之一。传

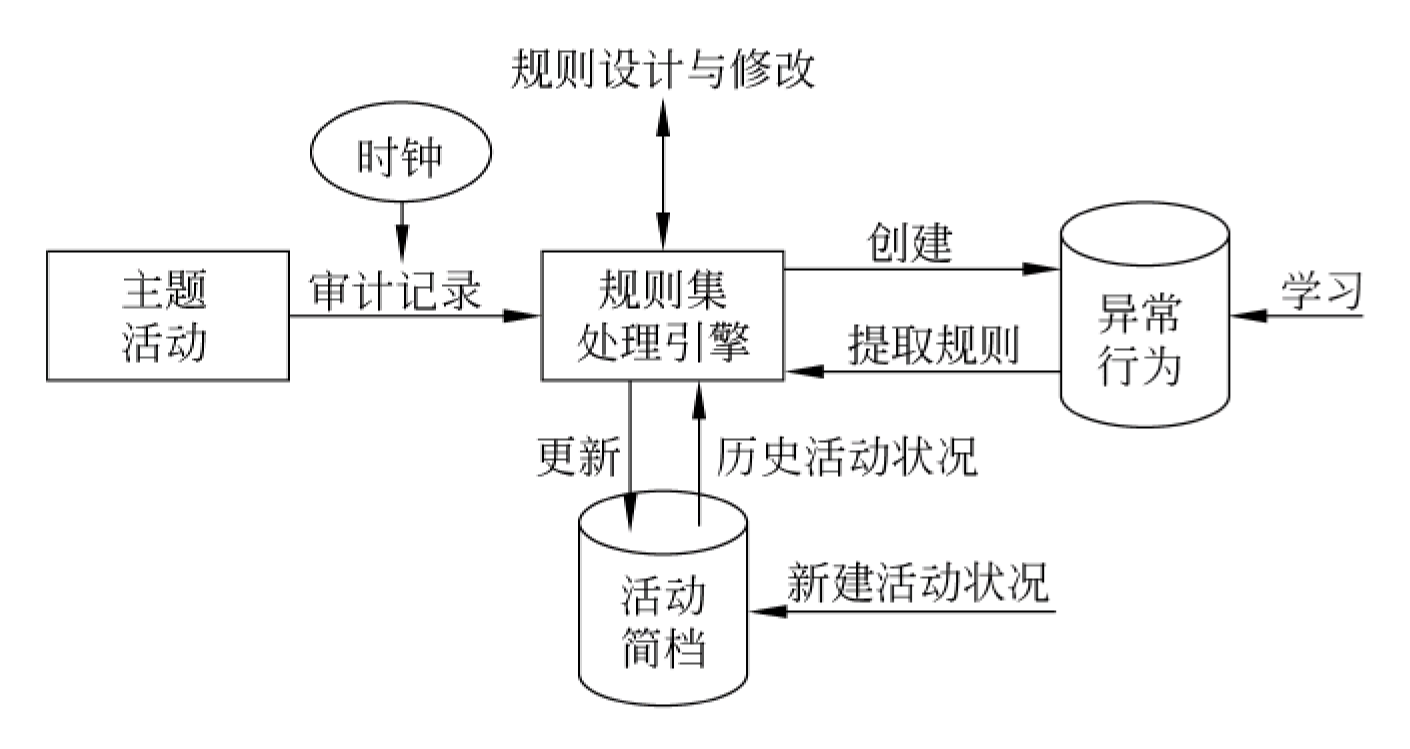



图 7-22 IDES 原型系统

统的操作系统加固技术和防火墙技术等都是静态安全防御技术，对网络环境下日新月异的攻击手段缺乏主动的反应。入侵检测技术通过对入侵行为的过程与特征的研究，使安全系统对入侵事件和入侵过程能做出实时响应。

入侵检测系统能完成如下任务。

(1) 监视、分析用户及系统活动，查找非法用户和合法用户的越权操作。

(2) 对系统构造和弱点的审计，并提示管理员修补漏洞。

(3) 识别反映已知进攻的活动模式并向相关人员报警，能够实时对检测到的入侵行为进行反应。

(4) 对异常行为模式的统计分析，发现入侵行为的规律。

(5) 评估重要系统和数据文件的完整性，如计算和比较文件系统的校验和。

(6) 对操作系统的审计跟踪管理，并识别用户违反安全策略的行为。

对一个成功的入侵检测系统来讲，它应该能够使系统管理员时刻了解网络系统(包括程序、文件和硬件设备等)的任何变更；为网络安全策略的制定提供指南；提供简单、方便的管理配置方法；入侵检测的规模应根据网络威胁、系统构造和安全需求的改变而改变；入侵检测系统在发现入侵后，应及时做出响应，包括切断网络连接、记录事件和报警等。

## 2. 入侵检测原理

入侵检测系统是根据入侵行为与正常访问行为的差别来识别入侵的，根据入侵识别采用的原理不同，可以分为异常检测、误用检测和特征检测三种。

1) 异常检测

进行异常检测的前提是认为入侵是异常活动的子集。异常检测系统通过运行在系统或应用层的程序来监控用户的行为，将当前主体的活动情况和用户轮廓进行比较。用户轮廓通常定义为各种行为参数及其阈值的集合，用于描述正常行为范围。当用户活动与正常行为有重大偏离时即被认为是入侵，如图 7-23 所示。如

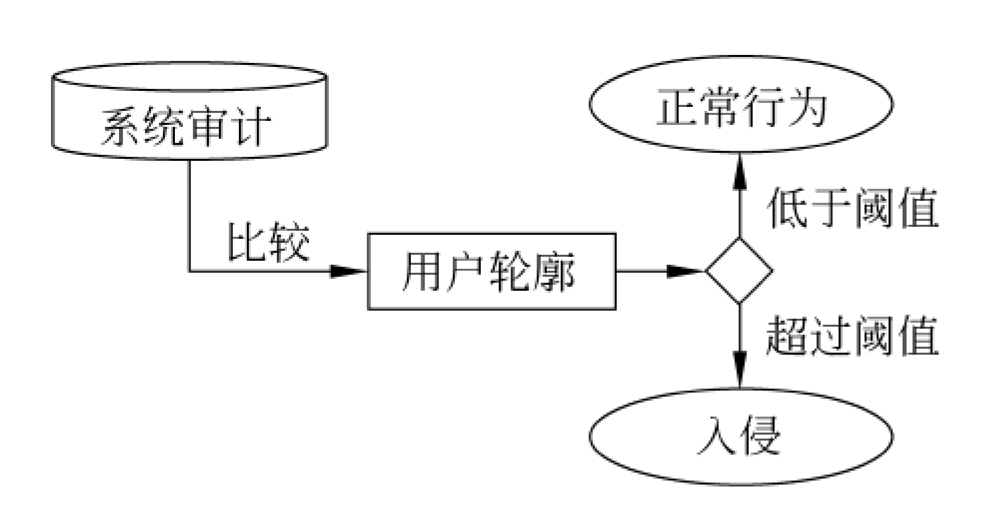



图 7-23 异常检测模型

果系统错误地将异常活动定义为入侵,称为错报;如果系统未能识别真正的入侵行为称为漏报。这是衡量入侵检测系统性能很重要的两个指标模型。

异常检测系统的效率取决于用户轮廓的完备性和监控的频率。由于不需要对每种入侵行为进行定义,因此能检测未知的入侵。同时系统能针对用户行为的改变进行自我调整和优化,但随着检测模型的逐步精确,异常检测会消耗更多的系统资源。

常见的异常检测方法包括统计异常检测、基于特征选择的异常检测、基于贝叶斯推理的异常检测、基于模式预测的异常检测、基于神经网络的异常检测、基于贝叶斯聚类的异常检测、基于机器学习的异常检测等。目前一种比较流行的方法就是采用数据挖掘技术来发现各种异常行为之间的关联性,包括源 IP 关联、目的 IP 关联、特征关联、时间关联等。

2)误用检测

进行误用检测的前提是所有的入侵行为都有可被检测到特征。误用检测系统提供攻击特征库,当监测的用户或系统行为与库中的记录相匹配时,系统就认为这种行为是入侵,如图 7-24 所示。如果入侵特征与正常的用户行为匹配,则系统会发生错报;如果没有特征能与某种攻击行为匹配,则系统会发生漏报。

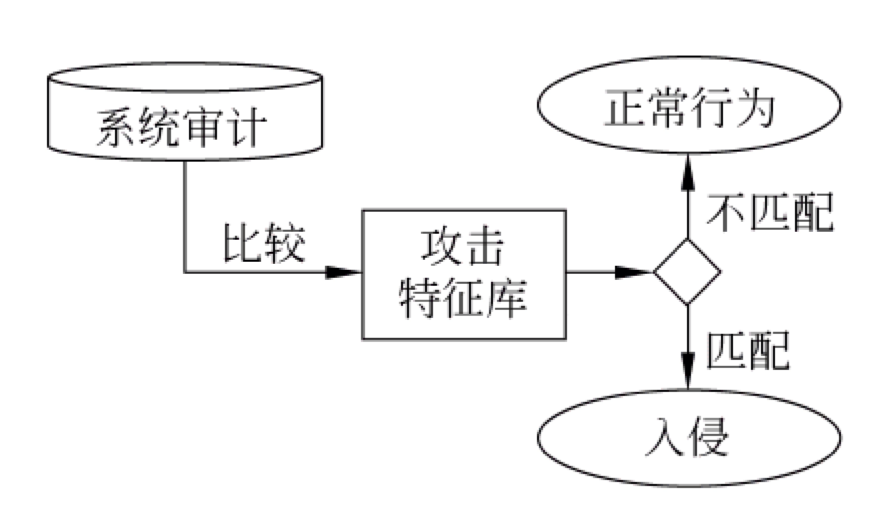


**图 7-24 误用检测模型**

采用特征匹配,误用模式能明显降低错报率,但漏报率随之增加。攻击特征的细微变化,会使得误用检测无能为力。

常见的误用检测方法包括基于条件概率的误用入侵检测、基于专家系统的误用入侵检测、基于状态迁移的误用入侵检测、基于键盘监控的误用入侵检测、基于模型的误用入侵检测等。

以基于条件概率的误用入侵检测方法为例,该方法将入侵方式对应于一个事件序列,然后通过观测事件发生情况来推测入侵出现。这种方法的依据是外部事件序列,根据贝叶斯定理进行推理检测入侵。

3)特征检测

和以上两种检测方法不同,特征检测关注的是系统本身的行为。定义系统行为轮廓,并将系统行为与轮廓进行比较,对未指明为正常行为的事件定义为入侵。特征检测系统常采用某种特征语言定义系统的安全策略。

这种检测方法的错报与行为特征定义准确度有关,当系统特征不能囊括所有的状态时就会产生漏报。

特征检测最大的优点是可以通过提高行为特征定义的准确度和覆盖范围,大幅度降低漏报和错报率。最大的不足是要求严格定义安全策略,这需要经验和技巧,另外维护动态系统的特征库通常是很耗时的事情。

由于这些检测各有优缺点,许多实际入侵检测系统通常同时采用两种以上的方法实现。

## 7.2.2 入侵检测分类

### 1. 基于主机的入侵检测系统

基于主机的入侵检测系统通过监视与分析主机的审计记录检测入侵。这些系统的实现不全在目标主机上,有一些采用独立的外围处理机,如 Havscack。另外 NIDES 使用网络将主机信息传到中央处理单元,但它们全部是根据目标系统的审计记录工作。能否及时采集到审计记录是这些系统的难点之一,从而有的入侵者会将主机审计子系统作为攻击目标以避开入侵检测系统。典型的基于主机的入侵检测系统模型如图 7-25 所示。

基于主机的入侵检测系统具有检测效率高,分析代价小,分析速度快的特点,能够迅速准确地定位入侵者,并可以结合操作系统和应用程序的行为特征对入侵进行进一步分析。但它也存在问题。首先它在一定程度上依赖于系统的可靠性,它要求系统本身应该具备基本的安全功能并具有合理的设置,然后才能提取入侵信息;即使进行了正确的设置,对操作系统熟悉的攻击者仍然有可能在入侵行为完成后及时地将入侵信息抹去,从而不被发觉。其次主机的日志能够提供的信息有限,有的入侵手段和途径不会在日志中有所反映。最后,在数据提取的实时性、充分性、可靠性方面,基于主机日志的入侵检测系统不如基于网络的入侵检测系统。

### 2. 基于网络的入侵检测系统

基于网络的入侵检测系统模型如图 7-26 所示,在共享网段上对通信数据进行侦听、采集数据并分析可疑现象。与主机系统相比,这类系统对入侵者而言是透明的。由于这类系统不需要主机提供严格的管理,因而对主机资源消耗少,并且由于网络协议是标准的,它可提供对网络通用的保护,而无须顾及异构主机的不同架构。基于网关的检测系统可以认为是这类系统的变种。

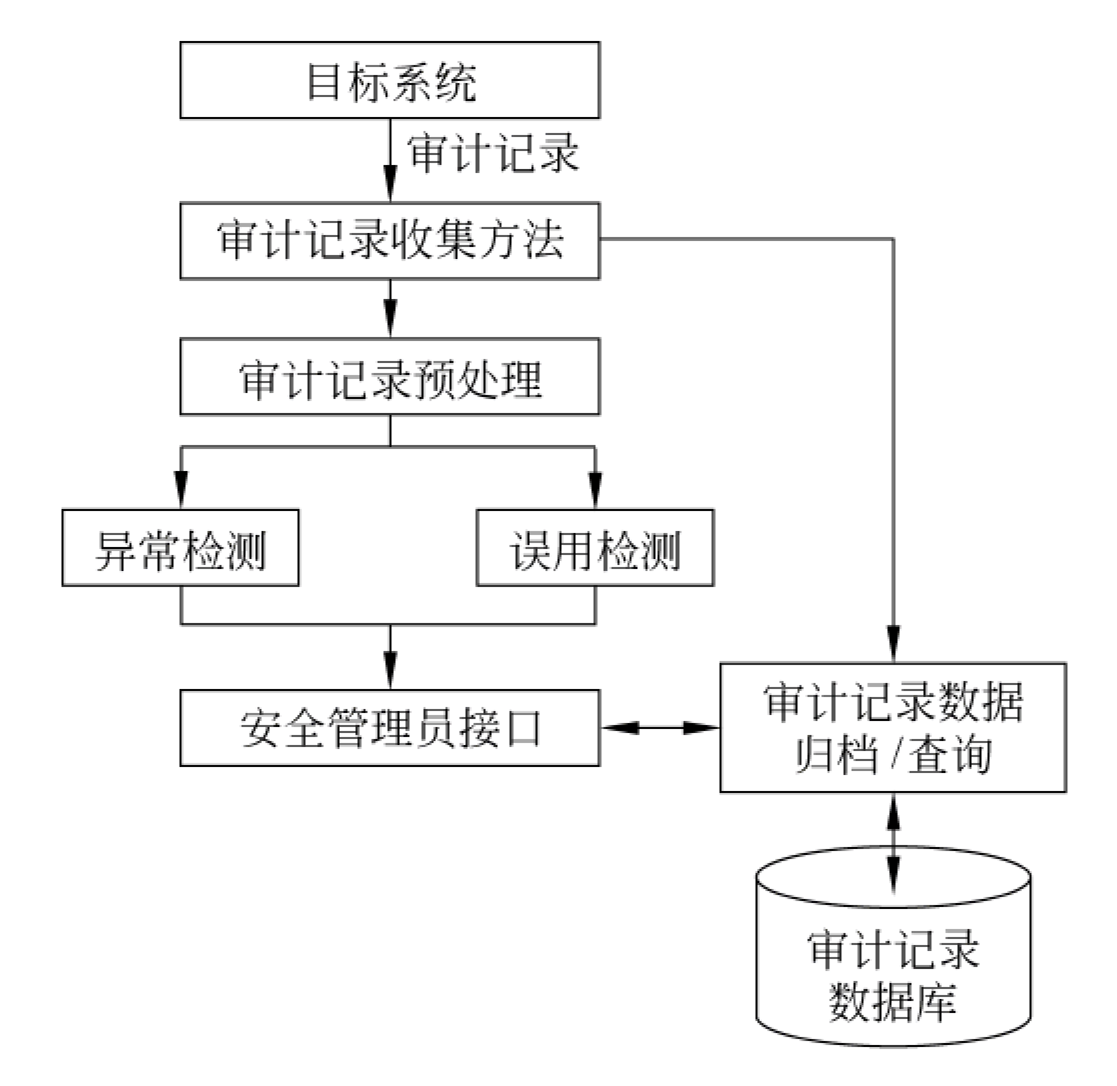



图 7-25 基于主机的入侵检测系统模型

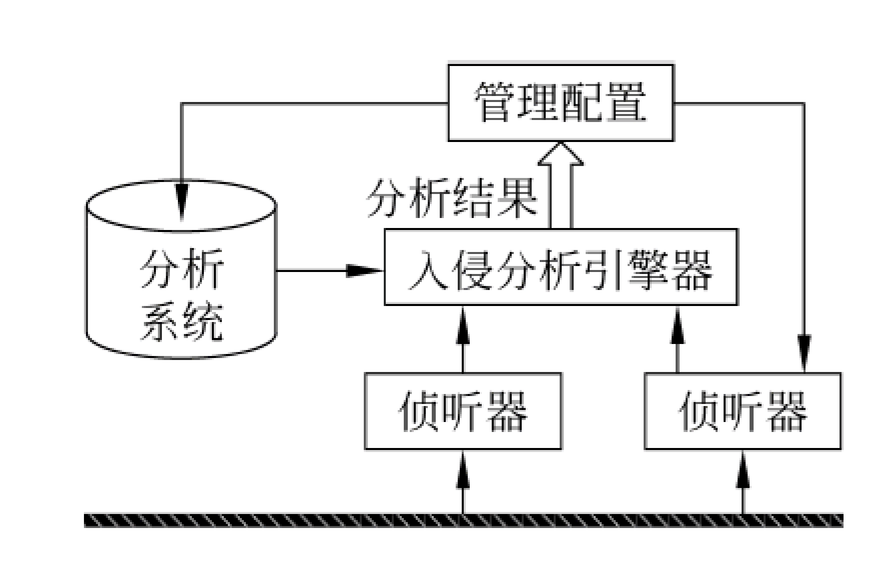



图 7-26 基于网络的入侵检测系统模型

网络入侵检测系统能够检测那些来自网络的攻击和超过授权的非法访问。网络入侵检测系统不和路由器、防火墙等关键设备以同样的方式工作,因此也不会成为系统中的关键路径,它发生故障不会影响正常业务的运行。

网络入侵检测系统只能检测与它直接相连的网段的通信,不能检测在不同网段的数据包。在使用交换式以太网的环境中就会出现监测范围的局限,而安装多台网络入侵检测系统的传感器会使部署整个系统的成本大大增加。同时,网络入侵检测系统为了性能目标通常采用特征检测的方法,它可以检测出一些普通的攻击,而很难实现一些复杂的需要大量计算与分析时间的攻击检测。网络入侵检测系统可能会将大量的数据传回分析系统中。在一些系统中监听特定的数据包会产生大量的分析数据流量。有些系统在实现时采用一定方法来减少回传的数据量,对入侵判断的决策由传感器实现,而中央控制台成为状态显示与通信中心,不再作为入侵行为分析器。

### 7.2.3 入侵检测技术常用的检测方法

入侵检测系统常用的检测方法有特征检测、统计检测与专家系统。目前入侵检测系统中绝大多数属于使用入侵模板进行模式匹配的特征检测系统,其他是少量采用概率统计的统计检测系统与基于日志的专家系统知识库系统。

#### 1. 特征检测

特征检测对已知的攻击或入侵的方式做出确定性的描述,形成相应的事件模式。当被审计的事件与已知的入侵事件模式相匹配时则立即报警。特征检测在原理上与专家系统相仿,在检测方法上与计算机病毒的检测方式类似。目前基于对包特征描述的模式匹配应用较为广泛。该方法预报检测的准确率较高,但对于没有先验知识(即专家系统中的预定义规则)的入侵与攻击行为无能为力。

#### 2. 统计检测

统计检测常用于异常检测,在统计模型中常用的测量参数包括审计事件的数量、间隔时间、资源消耗情况等。常用的统计入侵检测的五种模型为操作模型、方差、多元模型、马尔柯夫过程模型、时间序列分析。

#### 3. 专家系统

专家系统使用规则对入侵进行检测。所谓的规则就是知识,不同的系统与设置具有不同的规则,且规则之间往往无通用性。专家系统的建立依赖于知识库的完备性,知识库的完备性又取决于审计记录的完备性与实时性。入侵的特征抽取与表达是入侵检测专家系统的关键。在系统实现中,将有关入侵的知识转化为 if-then 结构(也可以是复合结构),条件部分为入侵特征,then 部分是系统防范措施。运用专家系统防范有特征入侵行为的有效性完全取决于专家系统知识库的完备性。

该技术根据安全专家对可疑行为的分析经验来形成一套推理规则,然后在此基础上建立相应的专家系统,由此专家系统自动进行对所涉及的入侵行为的分析工作。该系统

应当能够随着经验的积累而利用其自学习能力进行规则的扩充和修正。

## 7.2.4 入侵检测技术的发展方向

入侵检测技术的发展方向大致有以下几个。

### 1. 分布式入侵检测

传统的 IDS 局限于单一的主机或网络架构,对异构系统及大规模的网络检测明显不足,不同的 IDS 系统之间不能协同工作。为解决这一问题,需要发展分布式入侵检测技术与通用入侵检测架构。第一层含义针对分布式网络攻击的检测方法;第二层含义是使用分布式的方法来检测分布式的攻击,其中的关键技术是检测信息的协同处理与入侵攻击的全局信息的提取。

### 2. 智能化入侵检测

智能化入侵检测即使用智能化的方法与手段来进行入侵检测。所谓的智能化方法,现阶段常用的有神经网络、遗传算法、模糊技术等方法,这些方法常用于入侵特征的辨识与泛化。利用专家系统的思想来构建入侵检测系统也是常用的方法之一。特别是具有自学习能力的专家系统,实现了知识库的不断更新与扩展,使设计的入侵检测系统的防范能力不断增强,具有更广泛的应用前景。应用智能化的概念来进行入侵检测的尝试已经开始。较为一致的解决方案应为高效常规意义下的入侵检测系统与具有智能检测功能的检测软件或模块的结合使用。目前,尽管已经有智能化、神经网络与遗传算法在入侵检测领域的应用研究,但这只是一些尝试性的研究工作,仍需对智能化 IDS 加以进一步的研究,以解决其自学习与自适应的能力。

### 3. 应用层入侵检测

许多入侵的语义只有在应用层才能理解,而目前的 IDS 仅能检测如 Web 之类的通用协议,而不能处理如 Lotus Notes、数据库系统等其他的应用系统。

### 4. 高速网络的入侵检测

在 IDS 中,截获网络的每一个数据包,并分析、匹配其中是否具有某种攻击的特征需要花费大量的时间和系统资源,因此大部分现在的 IDS 只有几百兆的检测速度,随着千兆甚至万兆网络的大量应用,需要研究高速网络的入侵检测。

### 5. 入侵检测系统的标准化

在大型网络中,网络的不同部分可能使用了多种入侵检测系统,甚至还有防火墙、漏洞扫描等其他类别的安全设备,这些入侵检测系统之间以及 IDS 和其他安全组件之间如何交换信息、共同的协作来发现攻击、做出响应并阻止攻击是关系整个系统安全性的重要因素。例如,漏洞扫描程序例行的试探攻击就不应该触发 IDS 的报警;而利用伪造的源地址进行攻击,就可能触动防火墙关闭服务器,从而导致拒绝服务,这也是互动系统需

要考虑的问题。可以建立新的检测模型，使不同的IDS产品可以协同工作。

## 7.2.5 入侵防御系统IPS

### 1. IPS和IDS的关系

IPS到底是什么？“IPS可以阻断攻击，这正是IDS所做不到的，所以IPS是IDS的升级，是IDS的替代品”，可能很多人都会有这种看法。

我们先来看IPS的产生原因。

(1) 串行部署的防火墙可以拦截低层攻击行为，但对应用层的深层攻击行为无能为力。

(2) 旁路部署的IDS可以及时发现那些穿透防火墙的深层攻击行为，作为防火墙的有益补充，但很可惜的是无法实时地阻断。

(3) IDS和防火墙联动：通过IDS来发现，通过防火墙来阻断。但由于迄今为止没有统一的接口规范，加上越来越频繁的“瞬间攻击”(一个会话就可以达到攻击效果，如SQL注入、溢出攻击等)，使得IDS与防火墙联动在实际应用中的效果不显著。于是就有下面的一种想法，如图7-27所示。

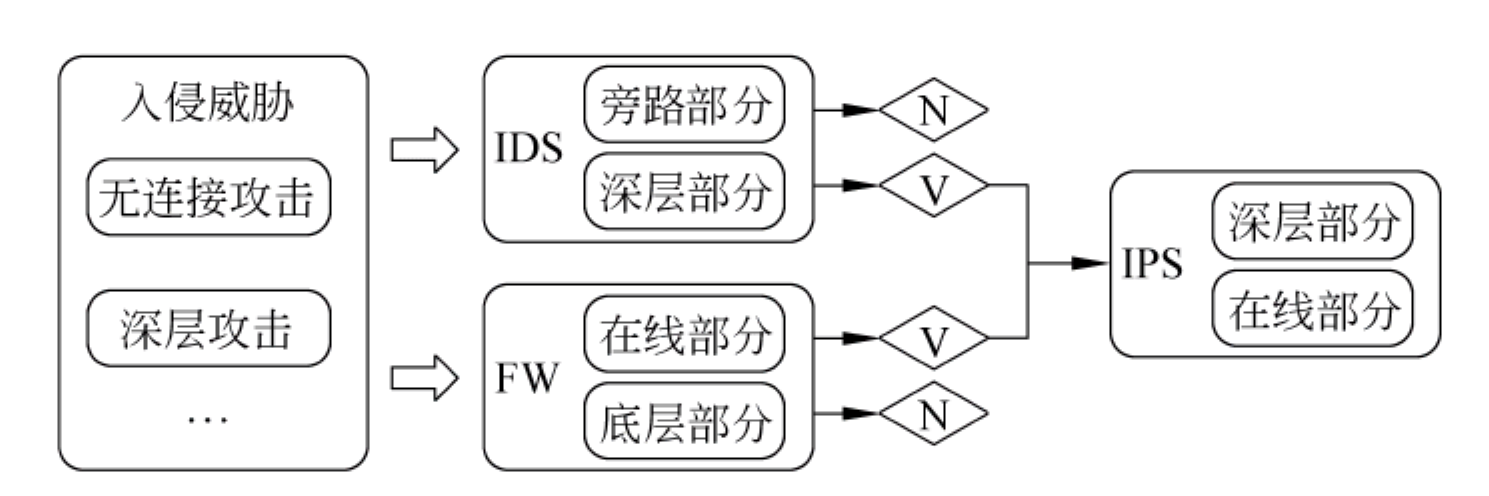



**图7-27 防火墙与IDS的缺陷引发IPS的产生**

这就是IPS产品的起源，一种能防御防火墙所不能防御的深层入侵威胁(入侵检测技术)的在线部署(防火墙方式)安全产品。

而为什么会有这种需求呢？是由于用户发现了一些无法控制的入侵威胁行为，这也正是IDS的作用。

入侵检测系统(IDS)对那些异常的、可能是入侵行为的数据进行检测和报警，告知使用者网络中的实时状况，并提供相应的解决、处理方法，是一种侧重于风险管理的安全产品。

入侵防御系统(IPS)对那些被明确判断为攻击行为，会对网络、数据造成危害的恶意行为进行检测和防御，降低或减免使用者对异常状况的处理资源开销，是一种侧重于风险控制的安全产品。

这也解释了IDS和IPS的关系，并非取代和互斥，而是相互协作。没有部署IDS的时候，只能是凭感觉判断，应该在什么地方部署什么样的安全产品，通过IDS的广泛部署，了解了网络的当前实时状况，据此状况可进一步判断应该在何处部署何类安全产品(IPS等)。

### 2. IPS 的性能

IPS 应该看重哪些方面的功能？有些人认为："IPS 应该具备各种扩展功能，ACL、路由、NAT 一个都不能少"。"IPS 最重要的就是性能了，其他的都不重要"。

入侵防御系统作为串接部署的设备，确保用户业务不受影响是一个重点，错误的阻断必定意味着影响正常业务，在错误阻断的情况下，各种所谓扩展功能、高性能都是一句空话。IPS 设备所应该关心的重点是精确阻断，即精确判断各种深层的攻击行为，并实现实时的阻断。

精确阻断解决了自 IPS 概念出现以来用户和厂商的最大困惑：如何确保 IPS 无误报和滥报，使得串接设备不会形成新的网络故障点？

而作为一款防御入侵攻击的设备，防御各种深层入侵行为是第二个重点。这也是 IPS 系统区别于其他安全产品的本质特点。同时也将精确阻断定义成保障深层防御情况下的精确阻断，即在确保精确阻断的基础上，尽量多地发现攻击行为（如 SQL 注入攻击、缓冲区溢出攻击、恶意代码攻击、后门、木马、间谍软件），这才是 IPS 发展的主线功能。

如何确保对深层入侵行为的准确判断？依托多年以来在入侵检测技术方面的深厚积累，一些入侵防御系统独创性地建立了柔性化检测机制，在确保精确判定攻击行为的基础上，涵盖了各种攻击手法类型。

常用的攻击检测方法有两种，一种方法是通过定义攻击行为的数据特征来实现对已知攻击的检测，其优势是技术上实现简单、易于扩充、可迅速实现对特定新攻击的检测和拦截。但仅能识别已知攻击、抗变种能力弱。另一种方法是通过分析攻击产生原理，定义攻击类型的统一特征，能准确识别基于相同原理的各种攻击、不受攻击变种的影响，但技术门槛高、扩充复杂、应对新攻击速度有限。两种检测机制如图 7-28 所示。

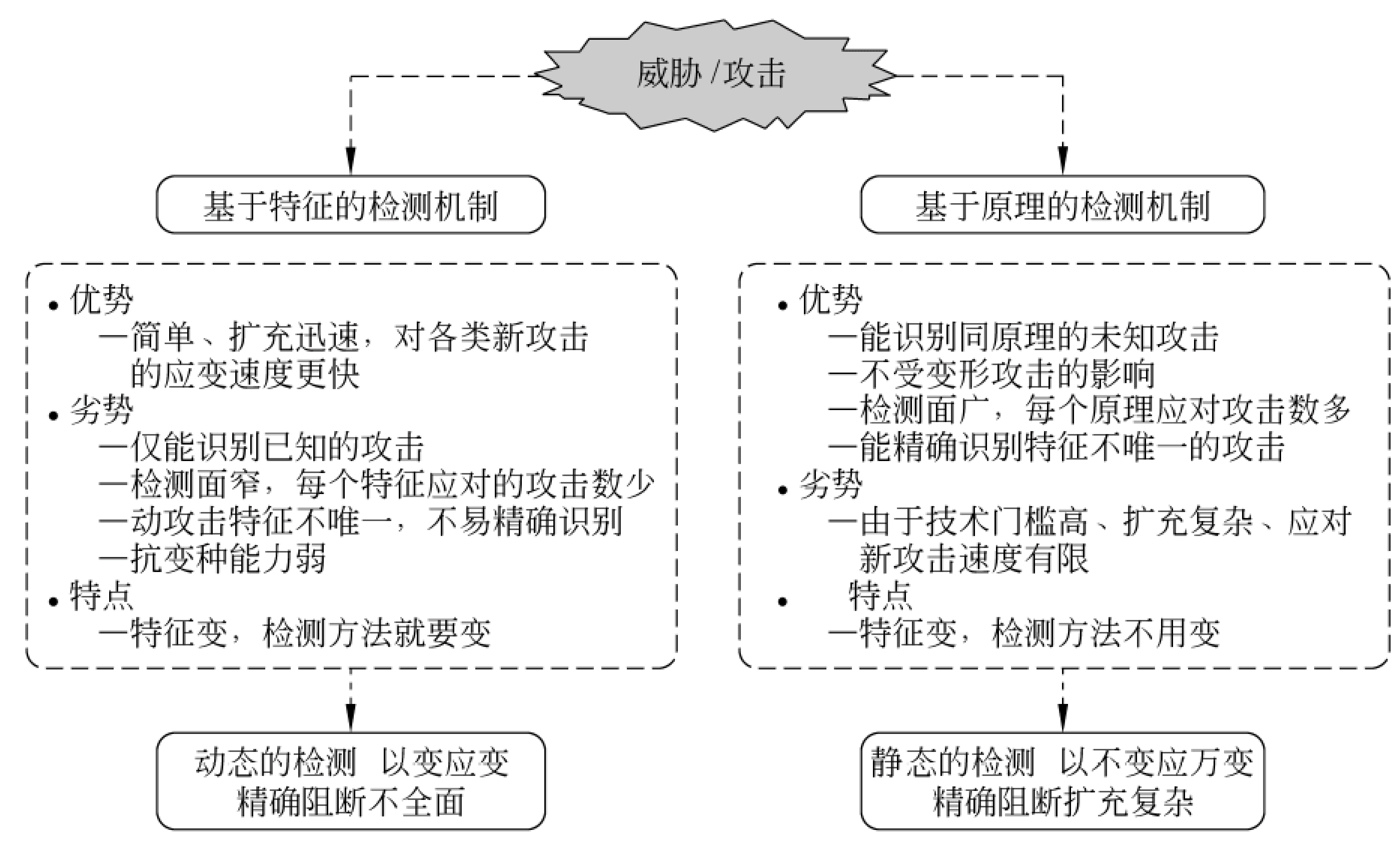



图 7-28 基于特征和原理的检测机制对比

融合“基于特征的检测机制”和“基于原理的检测机制”形成的“柔性检测”机制，它最大的特点就是基于原理的检测方法与基于特征的检测方法并存，有机组合了两种检测方法的优势。这种融合不仅是一个两种检测方法的大融合，而且细分到对攻击检测防御的每一个过程中，在抗躲避处理、协议分析、攻击识别等过程中都包含了动态与静态检测的融合，如图7-29所示。

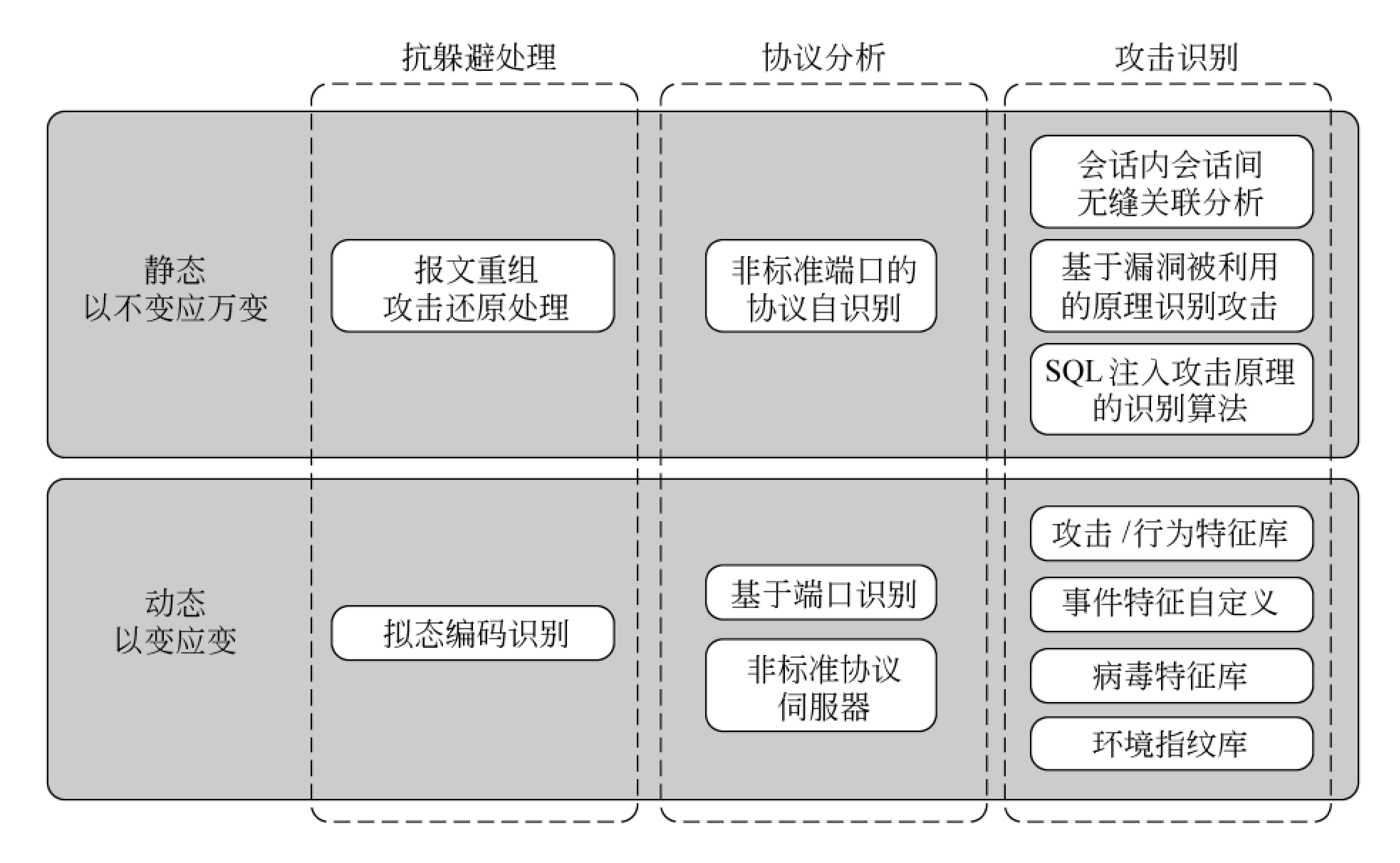



**图7-29 柔性检测机制原理**

通过运用柔性检测机制，一些入侵防御系统进一步增强了设备的抗躲避能力、精确阻断能力、变形攻击识别能力和对新攻击应变能力，提高了精确检测的覆盖面。

当然，前面提到的扩展功能和高性能，也是入侵防御系统所必须关注的内容，但也要符合产品的主线功能发展趋势，如针对P2P的限制。P2P作为一种新兴的下载手段，得到了极为广泛的运用，但由于无限制的P2P应用会影响网络的带宽消耗，并且还会带来知识产权、病毒等多种相关问题。而实现对P2P的控制和限制，需要较为深入的应用层分析，交给IPS来限制、防范，是一个比较恰当的选择。而ACL控制、路由、NAT等，这些都是防火墙可以完成的工作，在IPS上来实现这些功能，就有画蛇添足之嫌了。

性能表现是IPS的又一重要指标，但这里的性能应该是更广泛含义上的性能，包括了最大的参数表现和异常状况下的稳定保障。也就是说，性能除了需要关注诸如“吞吐率多大?”、“转发时延多长?”、“一定背景流下检测率如何?”等性能参数表现外，还需要关注“如果出现了意外情况，怎样/多快能恢复网络的正常通信?”，这个问题也是IPS出现之初被质疑的一个重点。串接设备出现故障和旁路设备不一样，是会影响到正常业务运营的，而做深层分析的串接设备更加如此，在长时间做大量数据深度分析的情况下，如何确保通信的顺畅？如何确保出现异常情况后通信的顺畅？

## 7.2.6 IDS与IPS的部署

从产品价值角度讲，IDS注重的是网络安全状况的监管。用户进行网络安全建设之前，通常要考虑信息系统面临哪些威胁，威胁的来源以及进入信息系统的途径，信息系统对这些威胁的抵御能力等方面的信息。在信息系统建设中和实施后也要不断地观察信息系统中的安全状况，从而有的放矢地进行系统建设，根据安全状况及时调整安全策略，减少信息系统被破坏的可能。

IPS关注的是对入侵行为的控制。当用户明确信息系统安全建设方案和策略之后，可以在IPS中实施边界防护安全策略。与防火墙类产品可以实施的安全策略不同，IPS可以实施深层防御安全策略，即可以在应用层检测出攻击并予以阻断，这是防火墙所做不到的，当然也是IDS所做不到的。

从产品应用角度来讲，为了达到可以全面检测网络安全状况的目的，IDS需要部署在网络内部的中心点，需要观察到所有网络数据。如果信息系统中包含了多个逻辑隔离的子网，则需要在整个信息系统中实施分布部署，以达到掌控整个信息系统安全状况的目的。

传统的IDS只能采用旁路方式检测网络攻击，不能实时阻断。当IDS检测到攻击时，入侵者的恶意企图往往已经得逞，系统或数据可能已被黑客控制或破坏，同时由于IDS处于旁路位置，检测的全面性和准确性也受到很大的影响。

而为了实现对外部攻击的防御，IPS需要部署在网络的边界，如部署在网关位置，利用攻击的知识对网络数据和行为进行深层检查，从而更有效地抵御应用层攻击。所有来自外部的数据必须串行通过IPS，IPS通过实时分析网络数据，发现攻击行为立即予以阻断，保证来自外部的攻击数据不能通过网络边界进入网络。

IPS在线的部署模式使它可以直接将有害的流量（探测、攻击等）阻挡于所保护的网络之外。IPS可以部署在防火墙之后，保护关键服务器并保证对外开放服务的安全（如Web、SMTP、DNS等）。FW＋IPS的部署模式充分发挥出FW和IPS各自的技术优势，并充分保护已有的安全投资。

明确了这些区别，就可以比较理性地进行产品类型选择。

若计划在一次项目中实施较为完整的安全解决方案，则应同时选择和部署IDS和IPS两类产品。在全网部署IDS，在网络的边界点部署IPS。若用户计划分布实施安全解决方案，可以考虑先部署IDS进行网络安全状况监控，后期再部署IPS。若用户仅仅关注网络安全状况的监控（如金融监管部门、电信监管部门等），只需在目标信息系统中部署IDS即可。图7-30是利用IDS和IPS联合部署用于防范DDoS的结构图。

合理地选择产品类型之后，下一个问题就是选择什么样的IDS或IPS才是最有效的？任何产品的开发应该围绕着核心产品价值展开，产品的各种能力都应该为核心产品价值服务。因此IDS必须能够全面检测网络中各类安全事件，也就是说检测的全面性是衡量IDS产品优劣的主要标准。而IPS必须能精确阻断关键网络威胁，对关键网络威胁的防御能力以及防御的准确性是衡量IPS产品优劣的主要标准。

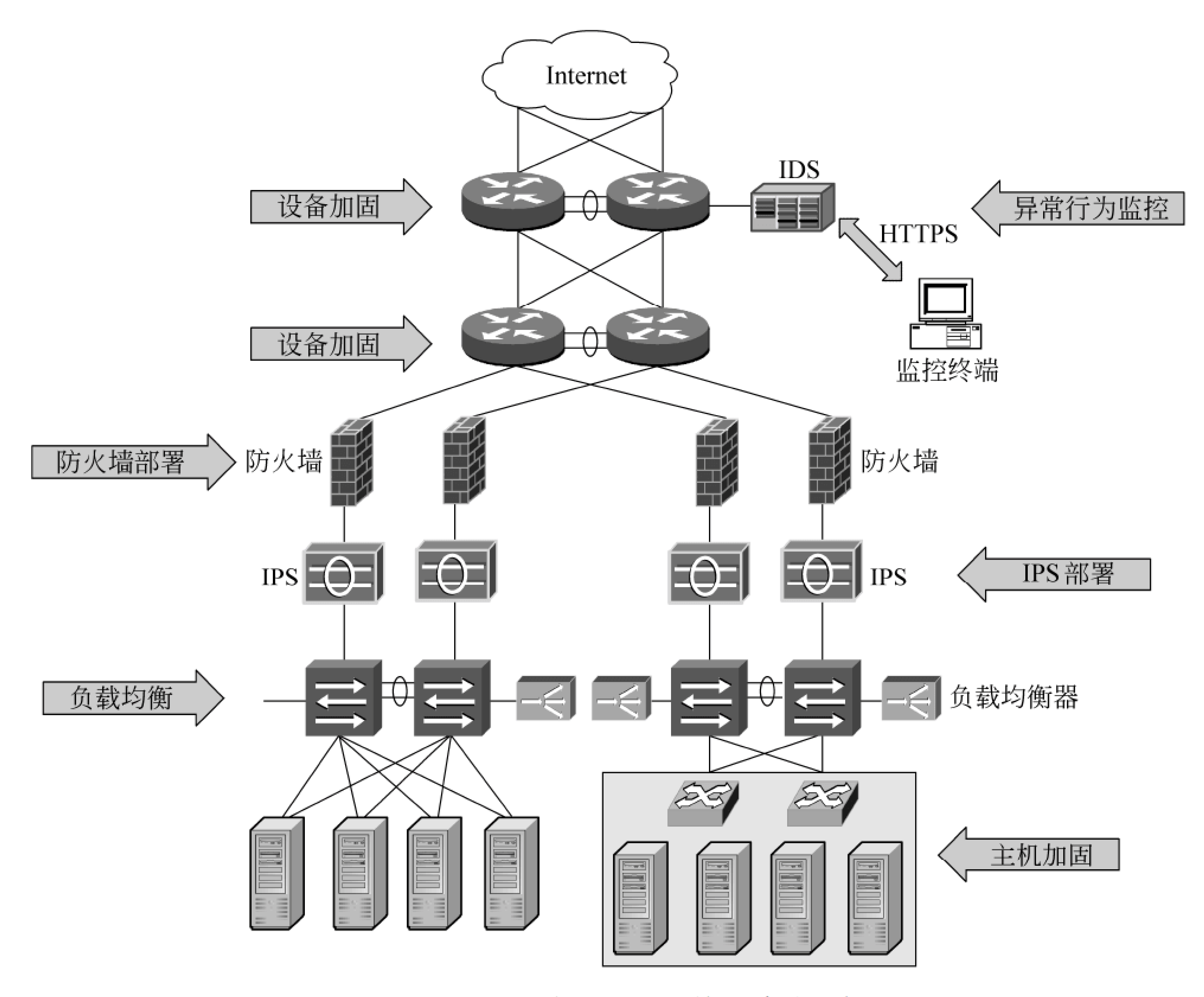



图 7-30 IPS 用于抵御 DDoS 的系统防御部署

## 7.3 身份认证

目前很多用户由于业务扩展,需要雇员能够在远程登录到内部网络并对网络资源进行访问。但是,无论这些雇员是以拨号方式连接、Telnet 方式连接,还是 VPN 方式连接,都涉及到一个不可回避的问题,就是如何对这些远程访问人员的身份进行认证,让他们能够有权限访问相应的资源。在目前网络安全环境下,不可能使用简单的账号和密码的方式,因为这涉及到防火墙、路由器的配置等许多问题。那么如何解决这类问题呢?可以在用户内部网设置一个服务器来分配证书,当访问某个资源时,要先对证书进行认证,再去访问资源。这个过程在网络安全中就称为身份认证技术。

身份认证是网络安全中的一个重要环节。在没有计算机的时代,身份认证可以通过眼睛的识别、接头暗号或者双方约定的方法进行。而在计算机时代,特别是计算机网络时代,人们很多交互都是通过计算机联网进行。这时,传统的人与人的交互分成了三个阶段:人与计算机交互、计算机与计算机交互以及计算机与人交互。在这些交互环节中的任何一个环节出现问题,则就会破坏人与人之间通过计算机网络的身份认证。

如图 7-31 所示,人与计算机之间的身份认证通常称为用户身份认证,传统上属于计算机安全研究的领域。而计算机与计算机之间通过网络进行身份认证通常称为报文身

份认证,传统上属于网络安全研究的领域。但是,目前一些研究者也从计算机网络环境下端到端的身份认证角度研究用户身份认证的技术,同样,也可以从网络环境的端到端用户身份认证角度讨论报文身份认证技术。所以,本节将在身份认证技术的应用中,具体讨论在网络环境下完整的用户身份验评过程。

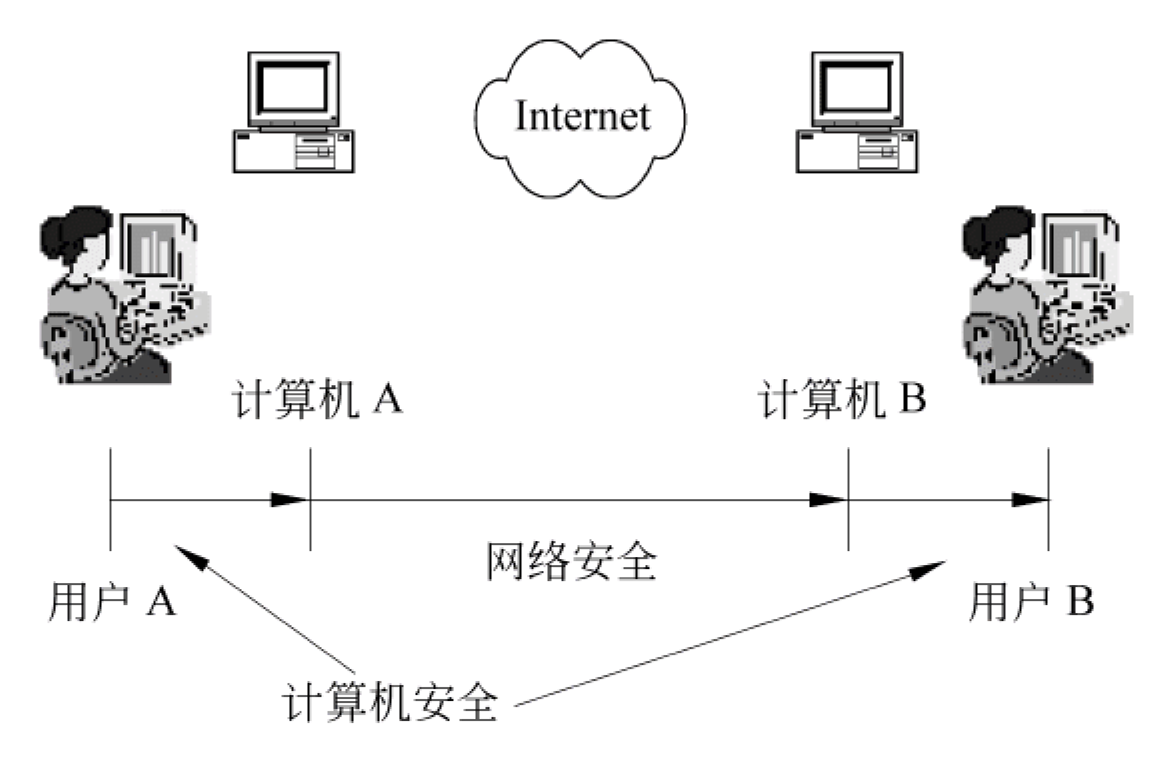



**图 7-31 计算机网络环境下人与人的身份认证**

## 7.3.1 身份认证的基本概念

身份认证是网络安全系统中的第一个环节,也是最重要的一个环节。没有身份认证,或者身份认证失效,也就无法在网络安全系统中进行访问控制和攻击检测。

**1. TCP/IP 体系身份认证的缺陷**

当前基于 IP 协议簇的 Internet 技术缺乏安全性,主要理由是这类 Internet 技术并没有设置有效的身份认证能力。为了说明为什么基于 IP 协议簇的 Internet 技术缺乏安全性,首先需要定义"身份认证"的概念。在网络安全环境下,"身份认证"是指对所有网络实体的标识和认证功能。而现在基于 IP 协议簇的 Internet 仅仅定义了网络实体的标识功能,没有定义网络实体的认证功能。现在的网络系统都是采用分层体系结构,目前实用的网络系统至少可以分成物理层、数据链路层、网络层、传输层和应用层。这五个层次的网络实体可以通过三类地址标识。

(1) 媒体访问控制(英文缩写为 MAC)地址,也就是网卡地址(俗称物理地址),标识了物理层和数据链路层实体,这是因为目前每个数据链路层实体都是对应一个媒体访问控制子层实体,每个媒体访问控制子层实体只对应一个物理层实体。

(2) 网络层地址,也就是 IP 地址,标识了网络层实体。这是 Internet 进行路由选择和报文转发的重要标识。

(3) 传送层和应用层地址,也就是 IP 地址+传送层端口号,标识了传送层实体。因为每个传送层实体唯一对应一个应用层实体,所以该标识也唯一标识了一个应用层实体。

但是,这些网络实体的标识都是在一定范围内可以随意设置的标识。例如,可以通过网卡相应的软件,重新设置 MAC 地址;可以在同一个子网范围内,重新设置 IP 地址;

既然可以重新设置 IP 地址，也就可以在不改变传送层端口号的情况下，重新设置传送层地址。之所以能够重新设置这些网络实体的标识，是因为这些网络实体标识都没有身份认证的能力，没有一种将每个网络实体的标识与该网络实体特征绑定的身份认证机制。这种简化的网络实体标识方法，虽然可以使网络互连、互通和互操作易于实现，但是使得在现有的 IP Internet 环境下无法有效地实施网络安全控制。

本节主要介绍网络环境下进行身份认证的原理和方法，再详细讨论现有的 IP Internet 是如何通过安全 IP 协议增加网络身份认证的机制。

### 2. 身份认证的发展历史

网络安全中采用的身份认证原理和方法来源于通信安全系统和计算机安全系统的身份认证技术。通信安全系统中的身份认证技术主要采用的是“安全身份认证协议”实现的一种技术。这是通过“质问－应答”交互过程实现身份认证的技术，类似于黑夜里的哨兵在看不清楚来人的情况下，通过询问“密码”识别来人的身份。

传统计算机安全中的身份认证技术主要是指多用户计算机系统中用户登录的密码系统。在多用户计算机系统中，每个用户都设置了一个账户，每个用户用自己账户登录到计算机系统时，必须输入与该账户匹配的密码。这里的账户就是用户的标识，而与用户账户匹配的密码，就是一种对用户身份的认证机制。

传统多用户计算机系统，曾经将用户的密码直接保存在计算机系统中，每次用户登录时，验证用户输入的密码是否与该用户账户存储的密码匹配。这种用户密码系统实际上是不安全的，如果攻击者获得存放用户密码的文件，则可以攻破整个系统。另外，系统管理员也可以访问用户密码文件，使得这种身份认证成为不可信的身份认证。

现在多用户计算机系统都不再直接存放用户密码，而是存放通过某个单向函数 $f$ 对用户密码 PW 的计算值 $f$(PW)。这里的“单向函数”表示在现有的计算条件下，无法从 $f$(PW)反推得出 PW 的函数。这样，即使网络攻击者获得用户密码文件，或者系统管理员访问用户密码文件，也无法获取用户的密码。而用户登录系统时，计算机系统不再直接比较密码，而是先将用户密码经过单向函数计算后，再与计算结果与给用户账户存放的密码函数值比较。如果匹配，则用户顺利通过身份认证，可以登录到计算机系统中。这种安全的计算机系统密码系统也被应用到网络安全中。

### 3. 身份认证的分类

计算机网络技术是通信技术与计算机技术结合的技术，同样网络安全系统中的身份认证技术也是通信系统身份认证技术与计算机系统身份认证技术结合的技术。

如图 7-32 所示，这是与图 7-31 类似的一种结构。只是这是使用网络服务的一种结构。在网络环境下，人们都需要通过某个计算机(即客户机 A)连接上网，然后通过网络与远程

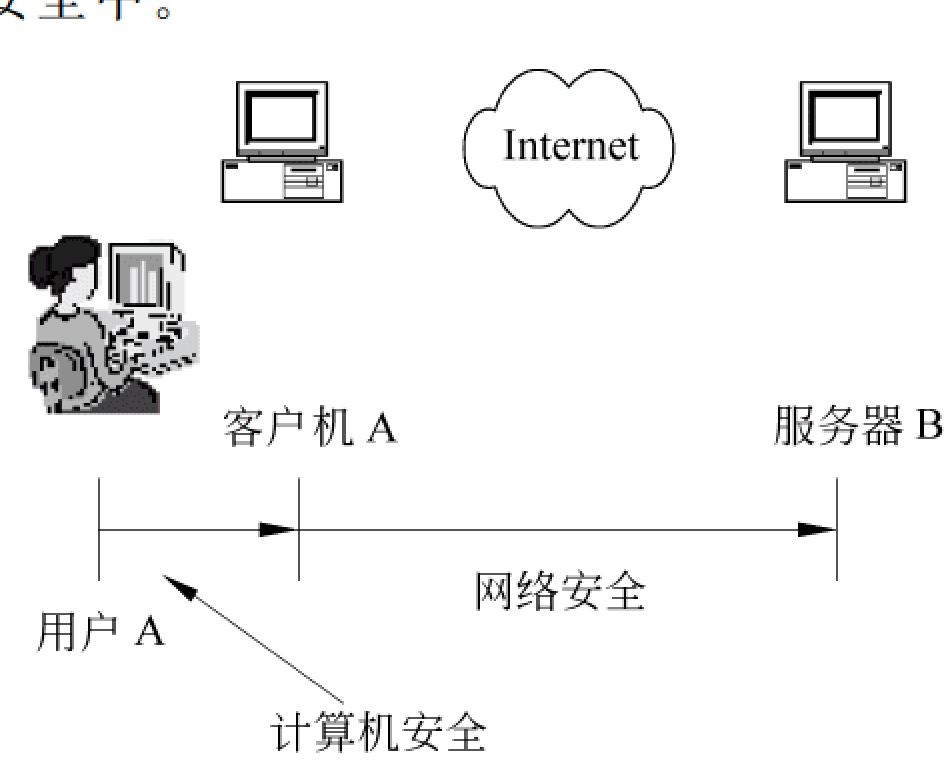



图 7-32 网络环境下的身份认证

一台提供网络服务的计算机(即服务器 B)交互。远程提供网络服务的计算机就是一台网络服务器,它可以同时支持多个用户的访问。网络服务器也相当于传统的多用户计算机系统。对于配置了安全控制功能的网络服务器,就需要使用多用户计算机系统中身份认证技术,即每个用户都需要设置账户和密码,登录到网络服务器中才能使用网络服务。

为了保证在客户机 A 和服务器 B 之间传递的报文不会被第三方攻击,A 和 B 之间就需要进行身份认证,A 需要确定 B 就是真实的服务器,而 B 需要确定 A 就是真实的客户机。这样,就需要利用通信安全系统中的安全身份认证协议。

基于以上网络环境中身份认证的特征,网络安全中的身份认证技术可以分成"人机交互类"身份认证技术和"报文传递类"身份认证技术。

1) 人机交互类身份认证技术

人机交互类身份认证技术是一种标识和认证网络服务使用者身份的技术,它是计算机安全系统的身份认证技术在网络环境下的具体应用。这类身份认证技术主要用于需要人参与的网络服务,例如电子邮件服务、文件传递服务以及 WWW 信息访问服务等。

网络安全系统中人机交互类身份认证技术,已经不再局限于传统计算机安全范畴中的人机之间的身份认证,而是扩展到通过网络实现人与人之间的身份认证。正如图 7-32 所示,人机交互类身份认证技术只是网络环境下身份认证技术的一个环节,它必须与报文传递类身份认证技术结合,才能构成跨越计算机网络的人与人之间的身份认证。从这个意义上看,人机交互类身份认证必须依赖于报文传递类身份认证。

2) 报文传递类身份认证技术

报文传递类身份认证技术是一种标识和认证网络中传递的报文身份的技术,它是通信安全系统的身份认证技术在网络环境下的具体应用。这类身份认证技术主要用于不需要人直接参与的网络报文的传递服务,例如网络层安全控制技术;安全 IP 协议以及传送层的安全控制技术;安全套接层(SSL)和传送层安全(TLS)协议。

表面上,报文传递类身份认证技术仅仅涉及到网络系统中计算机之间的交互。实际上,报文传递类身份认证建立的对报文发送方和接收方的信任,也是需要通过使用这些计算机的用户进行确认。所以,报文传递类身份认证技术需要依靠人机交互类身份认证技术,建立网络用户对报文传递的信任。

网络环境中真正完整的身份认证机制是包括了人机交互类身份认证技术和报文传递类身份认证技术的身份认证技术,下面介绍的 Kerberos 身份认证体系是一个典型的实例。

#### 4. 身份认证的方式

在网络安全中,根据身份认证参与方的数目,身份认证可以分成双方身份认证方式和三方身份认证方式。

双方身份认证方式是指在身份认证过程中,只需要涉及身份认证方和被认证方两个网络实体。双方通过交互身份认证协议,单向或者双向认证身份,如图 7-33 所示。单向身份认证指只有身份认证方认证对方的身份,双向身份认证指

被验证方 ←身份验证协议→ 验证方

图 7-33 双方身份认证方式

身份认证方和被认证方相互进行身份认证。

在人机交互类身份认证技术中,如果用户客户端软件需要与服务器端软件进行交互,完成身份认证的过程,则就是双方身份认证方式。如果用户客户端软件为了登录到服务器 B 中,还需要专门与另外一个身份认证服务器 C 交互,则就不是双方身份认证方式。

双方身份认证方式适用于身份认证双方处于同一个信任域的应用环境,即身份认证双方的行为不需要提交给第三方进行认证,不需要相互防范。所以,这种双方身份认证方式实际上不适用于电子商务环境。在这种身份认证方式下完成的身份认证,一旦出现商业交易纠纷,无法提交给第三方进行仲裁。

三方身份认证方式是指身份认证过程中,需要涉及到三个网络实体,其中包括身份认证的双方以及参与身份认证的双方都信任的第三方,如图 7-34 所示。在三方身份认证方式中,身份认证的交互双方需要通过作为公证方的第三方,才能相互认证身份。

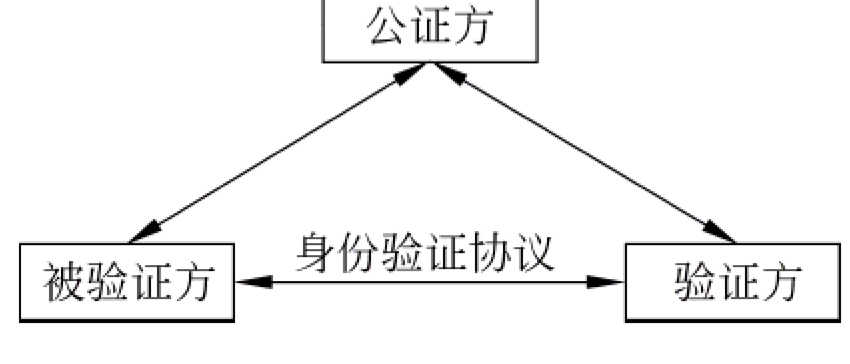



**图 7-34 三方身份认证方式**

在报文传递类身份认证技术中一种特殊的报文认证技术是数字签名技术,它就是采用三方身份认证的方式。报文发送方采用第三方发布的私钥加密报文摘要,而报文接收方采用第三方发布的公钥解密报文摘要。一旦出现双方争执,接收方可以将接收的报文提交给第三方进行认证,确定是否发送方发送的报文。

像"数字签名"这类三方身份认证方式已经广泛应用于电子商务领域,这种身份认证方式不需要双方彼此信任,只需要双方具有共同信任的第三方。

#### 5. AAA 认证体系

上述的身份认证技术,只解决了一个用户身份的确认问题,并没有将用户的身份与它能够访问的资源以及用户在获得身份确认后在网络上的操作活动联系起来,这对于当今网络应用的安全保证是远远不够的。因此,目前网络安全中建议采用认证、授权和记账系统,也被称为 AAA 系统。

(1) 认证,也称为身份验证,是指在做任何操作之前必须要识别操作者的真实身份,也就是"他是谁"。认证是一个过程,需要对用户提供的用户名和密码进行确认,只有在得到确认后,用户才能对网络服务器或硬件设备进行访问。

(2) 授权是指操作者到底有什么权限去进行操作,也就是"他能够做什么"。它是系统对用户定义的一种或多种安全策略的集合。这些策略可以定义到一个服务器上,对具有相应安全策略的用户进行授权,也可以定义到某个具体的设备上,对特定用户执行安全策略。

(3) 记账是指记录操作者的所有行为,即"他做了什么"。通过记账功能,管理员能够知道用户具体的操作,当然对入侵者的检测也可以通过记账功能来实现,这点在上节"入侵检测与防御系统"中已经做介绍。

由此可知,AAA 涵盖了对路由器、交换机、防火墙和服务器等硬件设备和软件的访

问控制策略,控制允许谁访问网络服务器以及允许使用何种服务。作为一个非常重要的框架,AAA 本身并不是协议,而是由 IETF 组织公布的标准,各实现厂商都要遵循这种标准来实现相应的访问协议。AAA 服务的网络如图 7-35 所示。

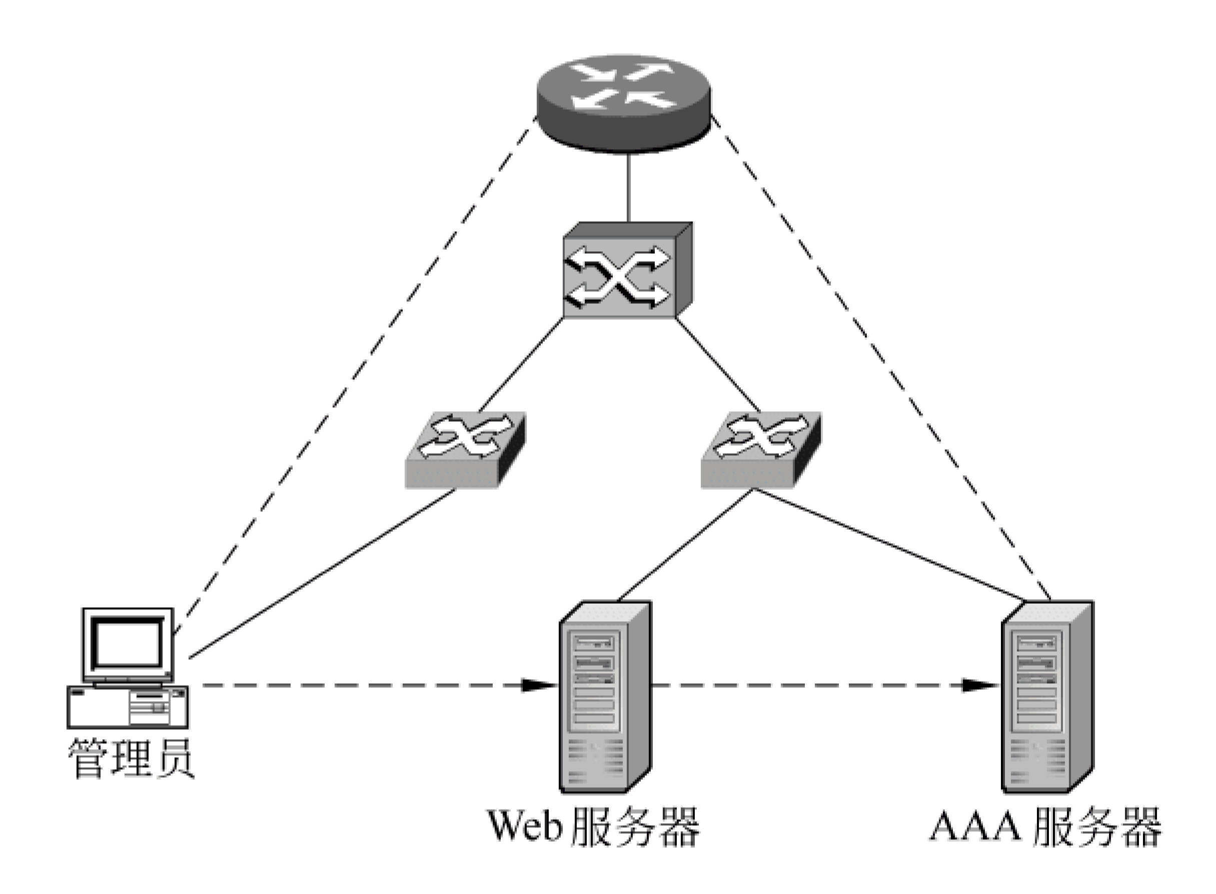



图 7-35 实用 AAA 服务的网络示意图

AAA 提供了访问控制的框架,使得网络管理员可以通过策略访问所有的网络设备。它具有如下的优点。

(1) 对安全信息,特别是账号等信息的集中控制。

(2) 扩展性强,安全产品厂商可以根据 AAA 规范设计生产自己的安全产品。

(3) 既适合于网络内部的认证也适合于网络接口的各种认证。

(4) 最大的灵活性,可对现有网络实施 AAA 框架而无须改造。

从图 7-35 中可以看出,网络上对路由器和服务器等网络资源的访问,都可以经过 AAA 服务器进行验证,而且只允许那些被授权的用户进行操作。也可以在网络中配置多个 AAA 服务器,并让它们协同工作。

AAA 最常使用的协议有 Kerberos、远程验证拨入用户服务(remote authentication dial-in user service,RADIUS)和终端访问控制器访问控制系统(terminal access controller access control system+,TACACS+)等。在本节中主要对 AAA 中的认证进行介绍,同时也会对常用的协议进行讲解。

## 7.3.2 身份认证的内容

前面已经提到了,认证是一个过程,它会将用户身份与一系列的认证证书进行比较来确认其正确性。这种认证的模式可以被各种各样的操作系统或应用程序使用。在通过认证以后,发起操作的主机或用户可以被授权来访问各种资源或信息。认证包括很多方面,下面对常见的认证方式进行讲解。

### 1. IP 认证

这种基于 IP 的认证,针对 IP 地址或 IP 子网信息,能应用到网络硬件设备上,如路由器或防火墙,其典型的应用有如下几种。

(1) 基于网络的应用程序,如 Linux 下的 rcmd. rsh 等命令。

(2) 基于 IP 或 DNS 的 Internet 应用程序,如 FTP 服务器或 Web 服务器。

(3) 像防火墙或路由器这样的访问控制设备。

IP 认证可以有效地将不符合规定的数据包阻止在网络之外,在前面的章节中讲到的 IPSec 就是基于 IP 认证的这种方式。IPSec 能够对在两个地址或路由器之间传输的数据包进行认证,如果符合定义的策略,则允许数据包的传输,否则将禁止传输数据包。但是 IP 认证也不是万能的,使用 IP 欺骗技术就可能会通过 IP 认证。

### 2. 基于账号的认证

基于账号的认证是最简单的,也是最常见的一种认证方式,大多应用在操作系统或应用程序上。它要求用户在登录操作系统或使用应用程序前,提供合法的账号及密码,如图 7-36 所示。

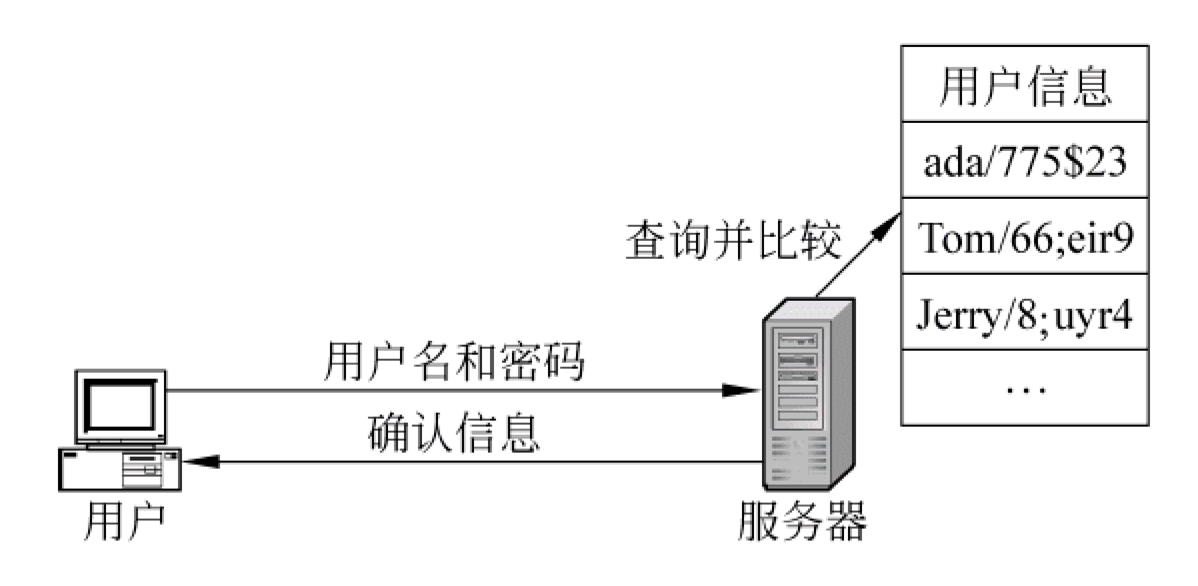



**图 7-36 基于账号的认证示意图**

从图 7-36 中可以看出,基于账号的认证方式有如下几个步骤。

(1) 用户在访问某台服务器时需要提供自己的账号和密码。

(2) 服务器在接到用户请求后,在自己的用户信息表或访问控制表中查找有无该用户。可有如下三种情况。

① 如果存在该用户信息,并且密码也正确,则接受这次访问。

② 如果存在该用户信息,但密码并不正确,则拒绝访问。

③ 如果不存在该用户信息,则拒绝访问。

(3) 将最终的确认信息返回给用户。

(4) 用户收到服务器的响应,如果是接受访问的话,就能与服务器之间建立连接并访问相应的资源。如果是拒绝的话,则不能访问相应的服务器和资源。

其实,这种认证方式也是最容易被破解的一种方法。如果黑客成功地将木马程序植入到目标主机,该程序会对用户的键盘操作或网络上传输的数据包进行监听并获得相关的信息。更严重的情况下,黑客会使用“暴力”(Brute-force)方法强行破解。这就要求采取必要的措施来保护账号及密码信息。

对信息内容的保护,最有效的方法就是对信息进行加密及校验,如图 7-37 所示。

数据加密标准(data encryption standard,DES)是较常用的一种加密方法,可以使用 56 位、64 位或 128 位密钥进行加密。密钥越长,破解起来就越困难,但处理数据所用的时间也会加长。当然随着计算机计算能力的增强,处理数据的时间将不会成为问题。加

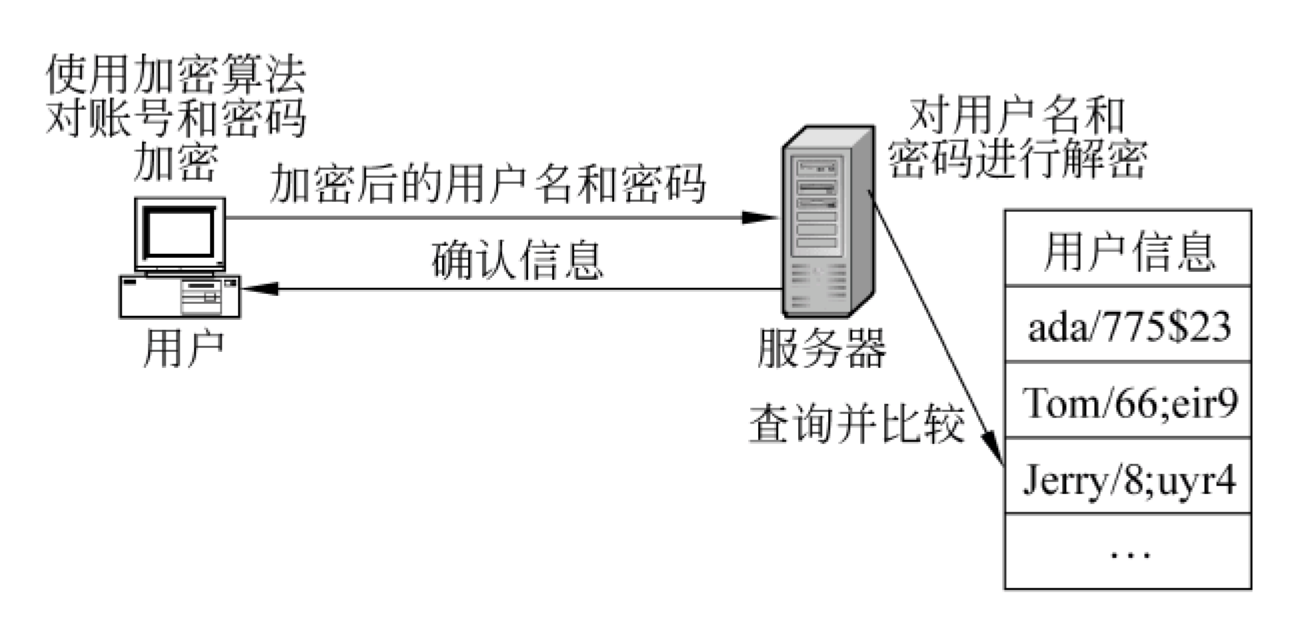



图 7-37 采用加密传输的方式

密算法分为对称加密和非对称加密等多种类型，具体加密方面的知识可参考有关密码学方面的书籍。

从图 7-37 中可以看到，相对于普通的账号认证，采用加密传输的方式分为两个步骤。

(1) 在客户端，用户需要采用某种加密算法对账号及密码进行加密。在网络传输的是密文，减少了数据被窃取的概率。

(2) 在服务器端，接到用户的数据包以后，首先要做的就是对数据包进行解密，将其还原成明文的形式。

这两个步骤可以增强数据的安全性。目前许多操作系统及硬件设备都支持加密的算法。例如 Linux/UNIX 系统采用 56 位的 DES 算法来保存用户账号及密码(账号及密码信息存放在/etc/passwd 文件中，密码是以加密的方式存储的)。

另一种有效的保护信息的方式是校验。常用的算法是消息摘要(message digest 5，MD5)，该算法对数据进行计算，得到一个 128 位的校验和(check sum)，如图 7-38 所示。

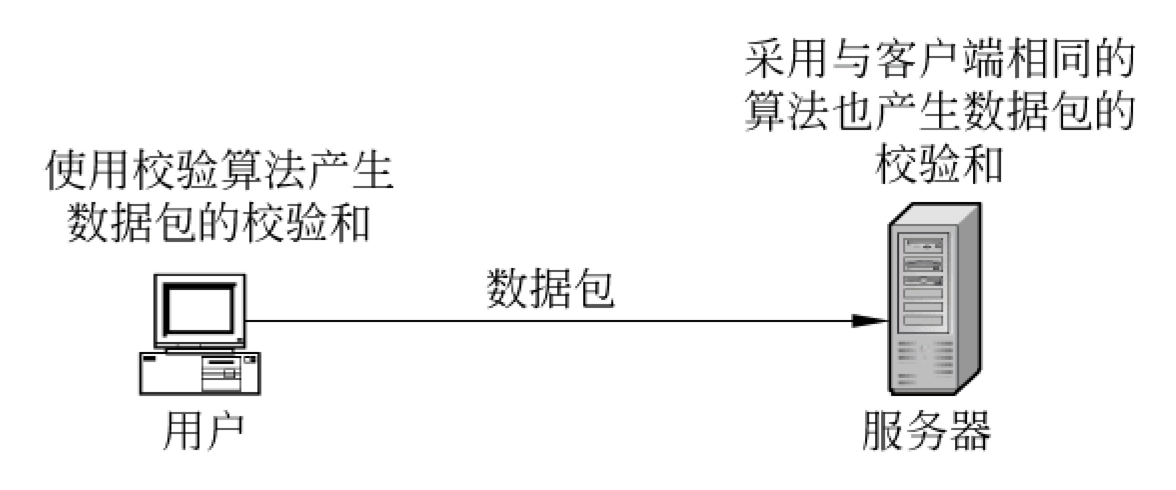



图 7-38 采用校验方式的数据传输

图 7-38 中显示了如何采用校验方式传输数据，它包含如下步骤。

(1) 客户端在传送数据包之前，先使用某种校验算法对数据包进行校验并生成校验和。当然这个校验和也要作为数据包的一部分传递给服务器端。

(2) 服务器端在收到数据包后，采用与客户端相同的校验算法再次进行校验并生成校验和。

(3) 服务器端将自己生成的校验和与数据包中的校验和进行比较。

① 如果一致，说明数据包在传输的过程中没有受到破坏，接受该数据包。

② 如果不一致，则说明数据包在传输的过程中已经受到破坏，将该数据包丢弃并向客户端发出一个通知。

当然，为了保证数据在网络传输过程中的高安全性，数据加密与校验方法通常是一起使用的，即先对数据包加密，再对加密后的数据包进行校验。IPSec 协议就可以使用这

两种方式的结合。

### 3. 基于令牌的认证

基于令牌的认证方式可以应用于防火墙、路由器或应用程序，证书（或令牌）既可以由硬件产生，也可以由软件产生。

这种认证方法可以提供很多安全特性，一旦用户成功登录到认证服务器，服务器就会为这次访问请求发布一个令牌，通过这个令牌，用户就可以去访问资源。当然，为了提高系统的安全性，该令牌可以是有时效性的，例如说60秒。超过这个时效，令牌就不能再使用，除非再次申请。因此，令牌认证方式可以看成是具有双保险的认证，需要提供两个重要的因素（Two-Factor），即用户的个人标识号（personal identification number，PIN）和服务器提供的处理方式。

图 7-39 给出了基于令牌的认证方式的过程，共有6个步骤。

图 7-39 基于令牌的认证方式过程

（1）客户端在访问网络资源前先访问认证服务器。

（2）如果认证服务器有该用户的信息，则认证服务器会向用户发放令牌。

（3）客户端使用此令牌去访问相应的应用服务器。

（4）应用服务器在收到用户的请求时并不能确认该令牌的有效性，需要将该用户信息及令牌再转交给认证服务器进行确认。

（5）认证服务器判断令牌的有效性，并将结果返还给应用服务器。

（6）应用服务器根据认证服务器的确认结果来决定用户的这次访问是否被允许。

### 4. 基于特征的身份认证

基于特征的身份认证，也就是根据被认证者“是什么”确定其身份。这种被认证者的“特征”通常是指不可假冒的、可以唯一标识被认证者的特征。在计算机安全中通常采用人体中不可假冒的、具有唯一性的生物特征，例如指纹和眼虹，进行基于特征的身份认证。这种身份认证不需要用户记忆数据，也不会丢失，是现有的身份认证技术中最为安全的一种身份认证技术。值得注意的，像指纹和眼虹这类人体生物特征，利用高技术是可以假冒的。

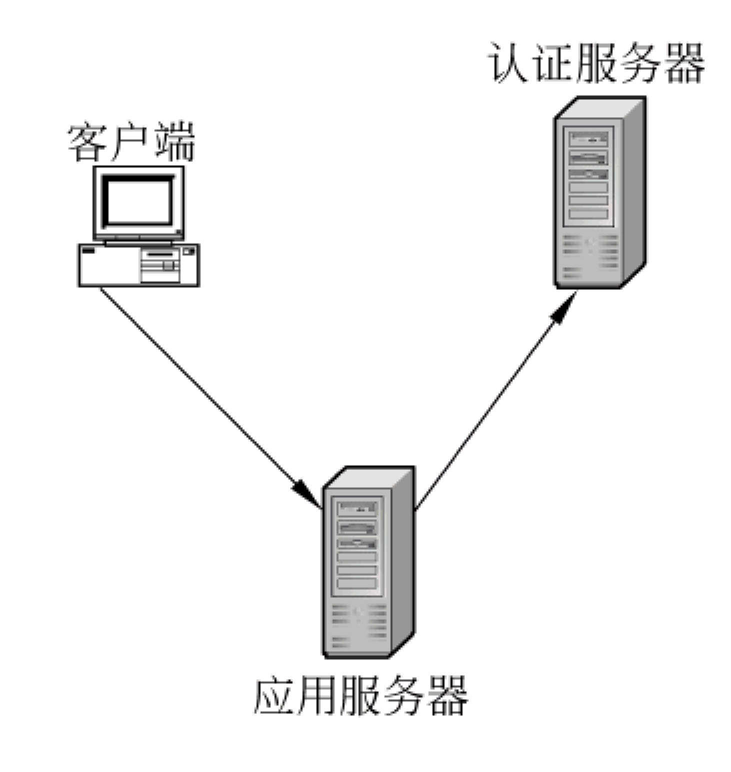


图 7-40 生物特征认证过程

在人机交互类身份认证技术中，基于特征的身份认证机制主要是指人体眼虹认证系统以及指纹认证系统。在报文传递类身份认证技术中，基于特征的身份认证机制主要是指基于“报文摘要”的报文认证码技术。“报文摘要”相当于一个报文的“指纹”，可以唯一地标识一个报文的特征。

图 7-40 所示为生物认证的过程，该过程包含如下几

个步骤。

(1) 用户的生物特性,如指纹等,存放在认证服务器中。

(2) 用户在登录时将手指放在指纹扫描器上。

(3) 用户的指纹被扫描并与认证服务器中的信息进行比较。

(4) 如果匹配的话,则用户身份被验证,并能够访问应用服务器。

### 5. 单点登录

在有些网络中,为了防止黑客得到管理员或用户的认证信息,通常会设置多个认证服务器。例如,用户要访问 DNS 服务器,需要提供一个账号和密码。如果想访问 Router,还需要提供另外一个账号和密码,即使这两个账号是相同的(谁会愿意去记多个账号和密码呢?)。

将所有的访问账号设置成唯一的值,在访问网络服务器时只需提供一个账号和密码,这种机制就是单点(single sign-on)。图 7-41 给出了 single sign-on 的工作原理,其基本思想如下。

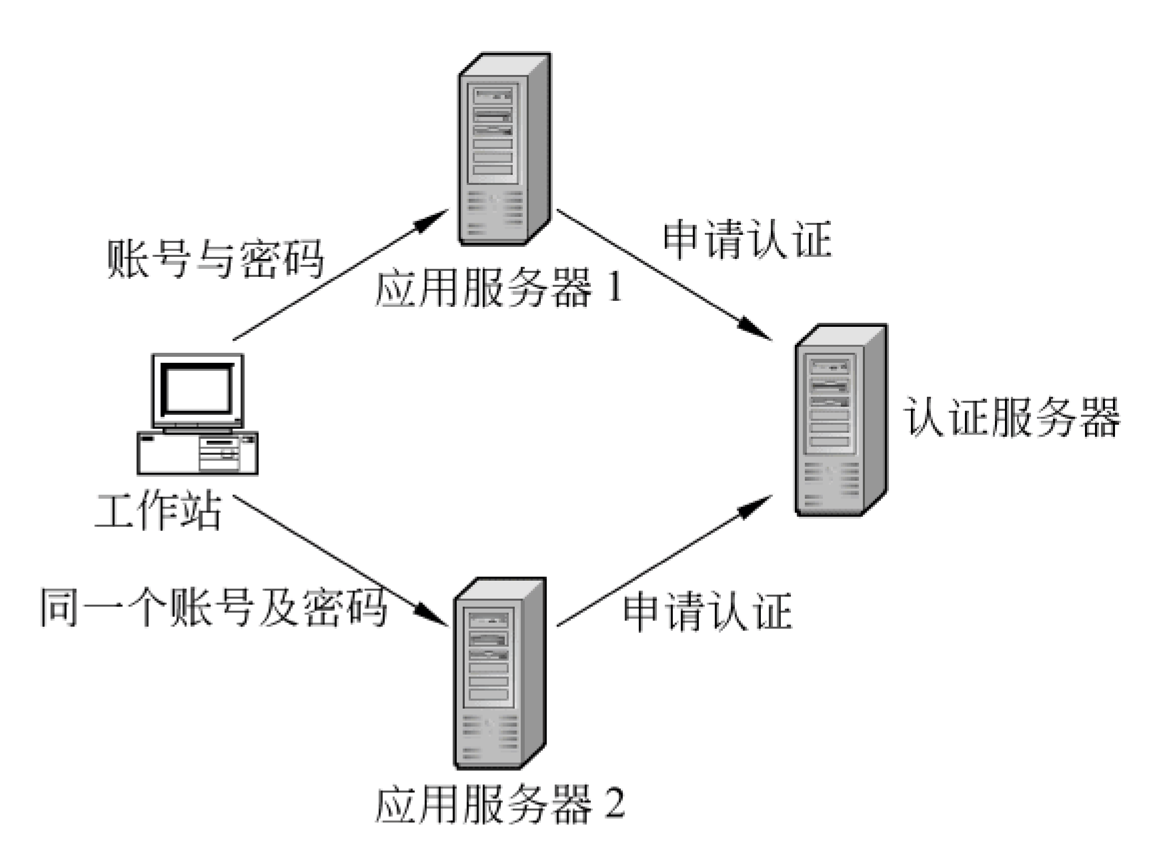



**图 7-41 single sign-on 原理**

(1) 用户的账号存放在认证服务器中,确保每个用户的账号是唯一的。

(2) 当用户访问应用服务器 1 时,该服务器使用认证服务器确认该用户的访问权限。

(3) 当用户访问应用服务器 2 时,使用相同的账号信息,该服务器也向认证服务器确认用户的访问权限。

单点登录的机制已经被广泛地使用,最著名的就是微软公司的 Passport。通过 Passport,用户提供一个有效的邮件地址,就可以访问相关的支持网站,当然也包括 MSN Messenger 这样的应用程序。这些网站或应用程序都到一个统一的认证服务器上验证用户信息。

### 6. 基于标志的身份认证

基于标志的身份认证,也就是根据被认证者"拥有什么"确定其身份。只要被认证者拥有具有"标志"意义的物品,例如银行发行的信用卡或者登录计算机系统的智能卡等,

就可以认证用户的身份，利用信用卡账号进行消费或者登录到智能卡指定的用户账户中。这种身份认证不需要用户记忆过多的数据，但是一旦这种“标志”物丢失，就很容易被他人假冒。例如一旦信用卡丢失，如果不及时挂失，自己信用卡账户中的钱就会被他人盗用。

在人机交互类身份认证技术中，基于标志的身份认证机制主要指采用身份识别卡的计算机或者网络登录系统。这种身份识别卡实际上就是存放了个人特有标志信息(例如个人特有的证书)一种存储介质，这种介质可以是个智能卡，也可以是直接接入 USB 端口的 U 盘。

在报文传递类身份认证技术，基于标志的身份认证机制主要指采用密钥的报文认证码技术。

以上介绍了身份认证的内容也可以简称为：所知(What you know)、所有(What you have)和所是(What you are)。由于单项内容难以保证身份认证的安全性，通常采用多项内容组合的方法进行身份认证以提供更加安全的机制。例如，通过 IP 的认证方式限制访问服务器的客户端，利用指纹作为用户的 PIN，一旦通过就对用户的这次访问发一个时效为 2 分钟的令牌等。或者采用“所知”加“所有”进行身份认证，持有身份标识卡的用户不仅需要插入标识卡，还需要输入密码，才能登录到计算机系统。再如采用“所知”加“所是”进行身份认证，用户不仅需要识别指纹，还需要输入密码，才能登录到计算机系统。在报文传递类身份认证中也应用了这种多项内容组合的方法，例如生成带有“保密字”的报文摘要作为报文认证码，这就是采用了“所知”加“所是”的身份认证方法。

### 7.3.3 Kerberos

Kerberos 协议是 20 世纪 80 年代由 MIT 开发的一种网络认证协议。该协议最初是基于 UNIX 系统的，在 RFC 1510 中定义了其内容。它允许一台计算机通过交换加密消息在整个非安全网络上与另一台计算机互相证明身份。一旦身份得到验证，Kerberos 协议给这两台计算机提供密钥，以进行安全通信。Kerberos 协议能验证用户的身份，并通过使用密钥加密的方式为用户间的通信提供安全性。

#### 1. Kerberos 的优点

Kerberos 是一种非常实用的认证协议，它有如下的优点。

(1) 服务器更加高效的验证。Kerberos 认证通过检查当前用户的信用证书验证客户。客户能够一次获得特定服务器的信用证书，并且在网络登录对话中再次使用它们。

(2) 相互验证。Kerberos 协议允许客户间、客户与服务器间或服务器间相互验证身份。

(3) 授权验证。Kerberos 协议有代理机制，它允许服务 A 在连接到其他服务如服务 B 时模拟服务 B 的客户，以访问相应资源或执行操作。

(4) 简化信任管理。Kerberos 协议使得多域网络不再需要明确的点到点的信任关系。每个域都将接受任何其他域发出的信任证书。

(5) 协同工作能力。

### 2. Kerberos 的认证过程

Kerberos 是一个三向的处理方法，它混合使用密钥加密和密码协议。根据称为密钥分配中心（key distribution center，KDC）的第三方服务来验证计算机相互的身份，并建立密钥，以保证计算机间的安全链接。KDC 由两部分组成，一个 Kerberos 认证服务器和一个证书授权（Ticket-granting）服务器。

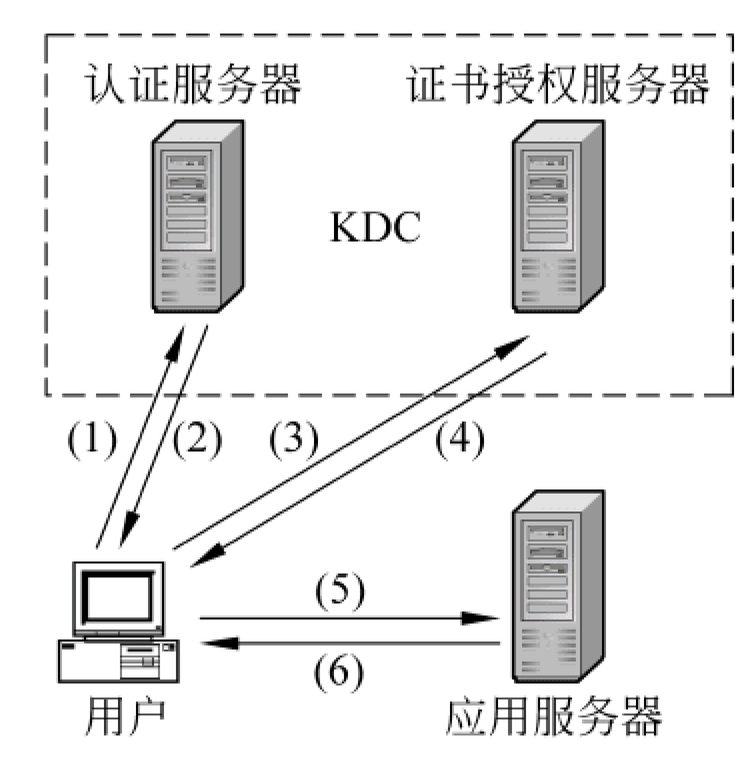


图 7-42　Kerberos 的工作原理

图 7-42 给出了 Kerberos 的工作原理，用户进行 Kerberos 认证需要 6 个步骤。

（1）用户向认证服务器发出请求，包括用户的身份、验证者名称、票据的有效期限等。

（2）认证服务器返回给用户响应，包括会话密钥、指定的有效时间和证书等。

（3）用户向证书授权服务器发出访问应用服务器的申请。此申请中包含会话密钥和证书。该密钥会与证书一起保存，以后用户再申请访问其他的应用服务器时不再需要提供自己的账号和密码。但这个密钥和证书是有时效的。

（4）证书授权服务器返回一个允许访问证书，允许用户对应用服务器的访问。

（5）用户向应用服务器出示自己的允许访问证书，并访问应用服务器。

（6）在用户的请求下，应用服务器有时也需要向用户证明自己的身份。当然此步骤是可选择的。

在第(2)步中，认证服务器返回给用户的响应信息是使用用户在认证服务器上注册的密码作为密钥来加密的。

## 7.3.4　RADIUS

RADIUS 协议最初是为拨号网络开发的，其目的是为拨号用户进行认证和记账，现已被广泛地应用于对网络设备的认证。

RADIUS 服务器具有对用户账号信息的访问权限，并且能够检查网络访问身份验证证书。如果用户的证书是可验证的，RADIUS 服务器则会对基于指定条件的用户访问进行授权，并将这次网络访问记录到记账日志中。使用 RADIUS 可以统一地对用户身份验证、授权和记账数据进行收集和维护，并集中管理。

RADIUS 一种基于询问/应答（challenge/response）方式的身份认证机制。每次认证时认证服务器端都给客户端发送一个不同的询问信息，客户端程序收到这个询问信息后，做出相应的应答。

### 1. RADIUS 的特点

RADIUS 的特点如下。

（1）RADIUS 采用 UDP 协议在客户和服务器之间进行交互，并符合 RFC 2856 规

范。RADIUS 服务器的 1812 端口负责认证,1813 端口负责计费工作。

(2) 采用共享密钥的形式。这个密钥不经过网络传播,而密码使用 MD5 加密传输。这样做可以有效地防止密码被窃取。

(3) 重传机制。能够在一个网络内设置多个 RADIUS 服务器,当某一个服务器没有响应时,用户还可以向其他的服务器发送询问请求。当然,如果 RADIUS 服务器的密钥和以前 RADIUS 服务器的密钥不同,则需要重新进行认证。

(4) 配置、使用简单。要使用 RADIUS,用户需要安装客户端应用程序,申请成为合法用户,并使用自己的账号进行认证。

**2. RADIUS 的认证过程**

图 7-43 所示为一个典型的 RADIUS 认证过程,它包括如下五个步骤。

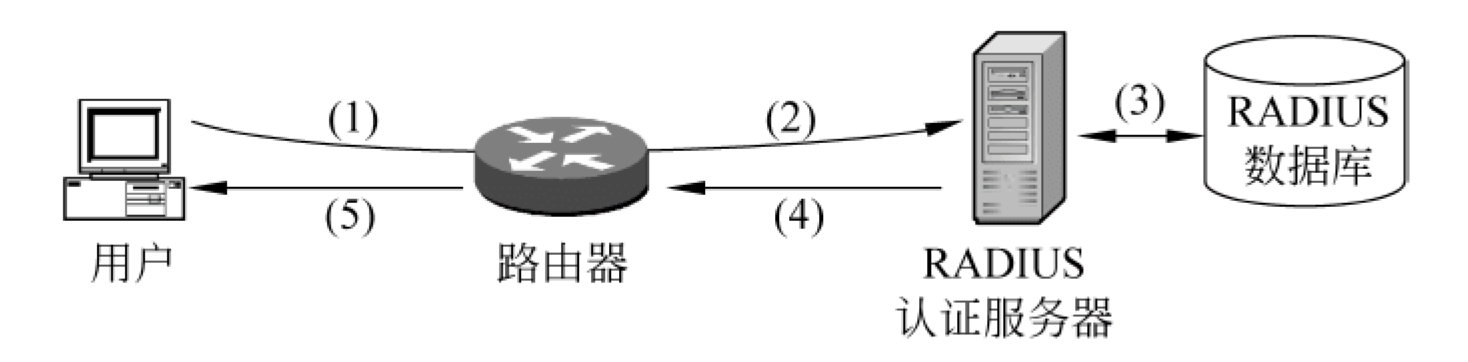



**图 7-43 RADIUS 的认证过程**

(1) 用户尝试登录路由器,提供必要的账号和密码信息。

(2) 路由器将用户信息加密,转发给 RADIUS 认证服务器。

(3) RADIUS 认证服务器在 RADIUS 数据库中查找相关的用户信息。

(4) 根据查找的结果向路由器发送回应。

① 如果找到匹配项,则返回一个访问允许(access-accept)消息。

② 如果没有找到匹配项,则返回一个访问拒绝(access-reject)消息。

(5) 路由器根据 RADIUS 认证服务器的返回值确定允许或拒绝用户的登录请求。

也可以在同一个网络中安装多个 RADIUS 服务器,这样可以提供更加有效的认证。

图 7-44 所示为一个多 RADIUS 认证服务器协同工作的过程,如果路由器在向 RADIUS 认证服务器 1 发送认证请求后,在一定时间内没有接到响应,它可以向网络中的另一台认证服务器,即 RADIUS 认证服务器 2 发送认证请求。依次类推,直到路由器从某个服务器得到了认证为止。当然,如果所有的认证服务器都不可用,那这次认证也就失败了。

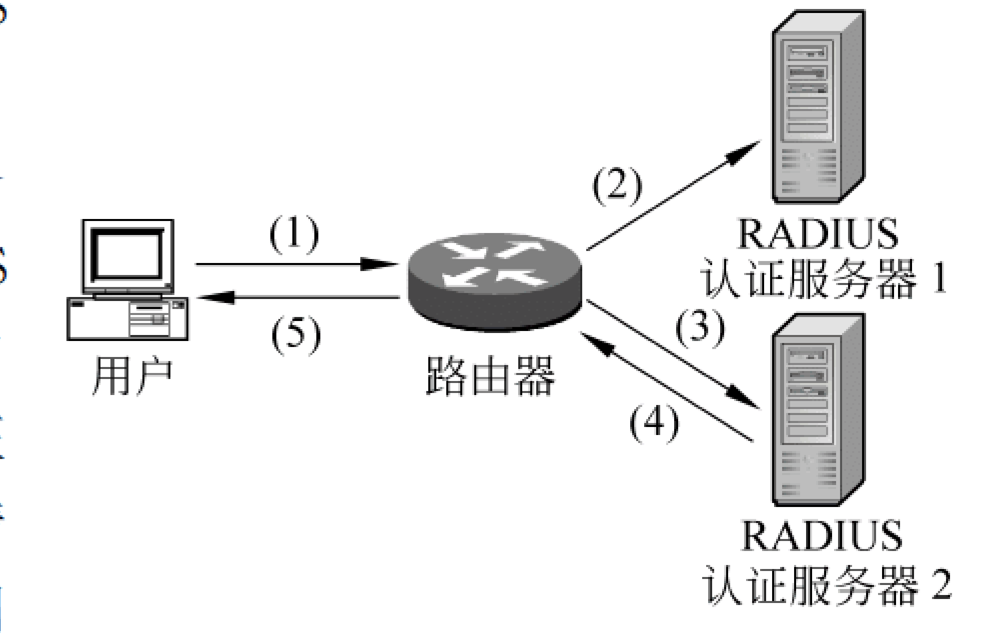



**图 7-44 多 RADIUS 认证服务器协同工作**

### 7.3.5 TACACS+

TACACS+是一种安全协议,能够为试图访问某个资源的用户提供集中的验证。最

早是由 Cisco 公司当做网络设备协议来开发的，但其规范已经成为工业标准。

TACACS+服务维护于一个数据库中，该数据库是由运行在 UNIX 或 Windows 上的 TACACS+守护进程管理的。TACACS+的服务是运行在 TCP 上的，默认端口是49。在使用 TACACS+的访问策略前，必须要对 TACACS+服务进行配置。

TACACS+提供了分离式模块化的认证、授权和记账管理。它为认证、授权和记账都单独设置了一个访问控制服务，也就是守护进程。每个守护进程在维护自己数据库的同时还能够充分利用其他的服务，无论这些服务是位于同一台服务器，还是分布在网络中。当然这依赖于守护进程的能力。

### 1. TACACS+的特点

TACACS+是通过 AAA 的安全服务来管理的，它能够提供如下的特点。

1）认证

通过登录和密码对话、询问和响应以及消息等方式，提供对认证管理的完全控制。

认证服务能处理与用户的对话。例如，当用户提供了账号和密码后，向用户访问诸如家庭地址、服务类型或社会安全号等问题。

TACACS+认证服务还能向管理所在机器发送消息。例如，通知管理员，由于公司安全策略的原因必须更改他们的密码。

此外，TACACS+协议还支持被访问资源与 TACACS+守护进程间的认证功能。

2）授权

在用户会话期间提供对用户操作能力的细粒度访问控制，包括设置自动执行的命令、访问控制、会话的持续时间或协议等。也可以限制用户在使用认证功能时允许执行的命令。

3）记账

收集用户记账、审计或报告用户的信息，并将它们发送到 TACACS+守护进程。网络管理员能使用记账功能跟踪用户的活动或提供用户的记账信息。记账信息由用户的身份、执行的命令、登录及退出时间、数据包的数量及数据包的字节等构成。

4）安全

在 TACACS+守护进程与网络设备之间的通信采用了加密的方式，对数据包的所有数据都进行加密，而不向 RADIUS 那样仅对密码加密。因此，TACACS+协议是安全的，至少到目前为止，还没有发布针对 TACACS+协议的安全警告。不过 TACACS+协议只是对网络设备与 TACACS+服务间的传输采用了加密的方式，并未对报文信息加密。黑客还是可以使用 sniffer 等软件探测相关的信息。

5）多种类型的验证方式

TACACS+可以使用任何由 TACACS+软件支持的验证，将多种验证方式结合起来，以提供最大的安全保护。

### 2. TACACS+的认证过程

当用户试图访问一个配置了 TACACS+协议的路由器时，开始的认证过程如下。

(1) 路由器在用户与 TACACS+守护进程之间建立连接并传递消息。这是一个交互的过程,路由器从守护进程那里得知需要用户提供什么样的信息并返回给用户,用户按要求填写完毕后,再经路由器传送给 TACACS+认证服务器。如此反复直到 TACACS+守护进程得到了所有必要的认证信息为止。通常认证信息包括用户名、密码、家庭住址等。

(2) TACACS+守护进程根据认证信息的结果向路由器发送响应。响应包括如下4种。

① ACCEPT:认证成功,可以接着做其他的事情。

② REJECT:认证失败,拒绝用户的访问。

③ ERROR:在认证的过程中出现了错误,认证终止。

④ CONTINUE:需要用户提供额外的认证信息。

(3) 认证成功后,还需要进行 TACACS+授权。这依然需要路由器与 TACACS+守护进程建立连接,守护进程会返回下列两种类型的响应。

① REJECT:拒绝访问。

② ACCEPT:允许访问。用户可以对路由器执行一些操作。

## 7.3.6 身份认证管理

### 1. 产生身份认证管理的需求

有了身份认证系统,但随着应用系统不断增多以及用户雇员流动增大,网络管理人员还会遇到两个很头痛的问题:一是在为新员工创建新账户,激活所有他可以使用的资源时,需要多长时间?二是当有员工离职时,能在多短的时间内将他的所有账户清除?

当企业的员工人数不多、IT 应用也不多的时候,上面的问题也许不难,但当企业规模达到一定程度,企业内部的“信息孤岛”带来的将不只是信息沟通困难。会发现原来存在于各个独立系统中的资源访问权限管理和身份认证管理仍然是“各自为政”。当网络中添加的资源越多,就越难加以控制,从而导致出现各种不安全可能。新的基于身份认证(Identity-based)管理技术的兴起将有助于理顺网络秩序,下面将从不同的层面来诠释身份认证管理的发展现状。

部署基于身份认证管理的 IT 基础架构是今后的大方向。更重要的是数字化的身份认证管理正在从安全到服务配置的各个层面改变网络的外观和内在管理机制。

传统的企业安全模型是通过对少量数据中心进行参数化实现的,但这种方式已经无法满足业务增长过程中遇到的适应性和扩展性需求。而新的基于身份认证的访问系统能够在帮助企业管理好复杂网络的同时,使得系统安全能够与其商业目标更加接近,而不仅仅是从 IT 的角度考虑系统该如何管理。像 IBM、Novell、Netegrity、Oblix 等厂商现在都提供相应的身份认证管理(Identity Management)解决方案。

身份认证管理技术已经在单点登录(single sign-on,SSO)领域成功应用,但其实 SSO 只是它的应用之一,基于身份认证管理的网络管理才是它今后更为宽广的发展方向。

“企业在身份认证管理上的投资正使以身份认证为中心的网络管理成为可能。”

Burton 集团副总裁兼目录和安全战略部门服务总监 Phil Schacter 如是说。他特别指出,当今网络在移动性和远程访问方面能力的增强逐渐成为网络管理向基于身份认证系统迁移的驱动力量。

身份认证管理系统不仅定义了用户是谁,而且把“谁”与“什么”直接联系在一起。例如用户在组织中的角色是什么?用户需要访问什么资源和信息?他/她能够对信息进行什么操作,不能进行什么操作?身份认证提供了一个整体视图,使企业的策略和流程一致地应用于整个企业当中,其工作原理如图 7-45 所示。

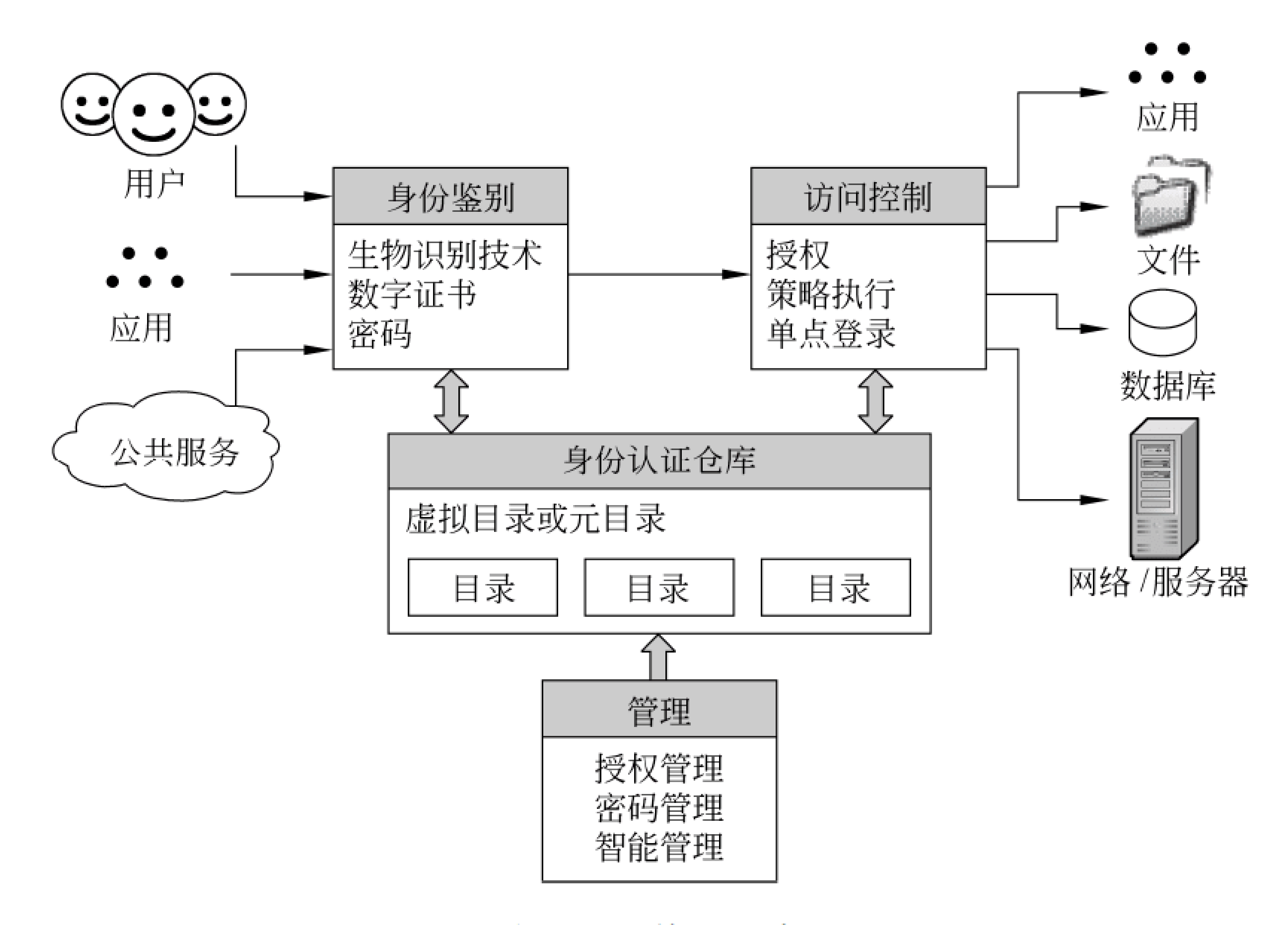



**图 7-45　身份认证管理系统工作原理**

通过强化管理每个用户的访问与授权信息,身份认证管理解决方案使得网络能够保持最新状态,新员工能够迅速访问企业内外部网络。无用账户将被尽快清理,以免离职员工利用其旧账户进行非法操作。它还能提供审核信息,确保企业对管理法规条例的遵守。并能保护员工隐私和加强访问控制。最重要的是基于身份认证的网络管理使得安全脱离了数据中心,而且它基于角色管理的方式使得网络管理与企业的业务需求更相符。

**2. 先集成目录**

将自己的网络管理系统向基于身份认证的网络管理迁移时要求很苛刻,但这并不意味着彻底推翻原有的软件基础架构。相反,身份认证系统能够使现有的基础架构更加强壮和智能化,并且更易于防范未经授权的访问企图。

要做的第一步工作就是建立身份认证仓库(identity storehouse),将用户的访问信息独立于应用程序来进行集中管理。典型的形式是采用网络目录,如 LDAP 目录、微软的活动目录、Novell 的 eDirectory 等。

事实上现在很多组织已经维护有多个网络身份认证信息目录,并且拥有多个合作伙

伴、供应商和客户的数据库,里面常常包含有重复的、非公共的数据。也就是说目录也需要集成。

目前正在形成的两类目录集成工具能够担此重任。例如 Novell Nsure Identity Manager 这样的元目录(metadirectory)解决方案就可以建立单一的权威目录作为所有数据的数据源。另一方面,像 OctetString Virtual Directory Engine 这样的虚拟目录产品能够提供虚拟的单一数据库,但实际上它是从各个数据源抽取数据,并使数据显示来自同一位置。在企业选择建立身份认证仓库的工具时,需要考虑已有的组织架构,没有哪种方式拥有绝对优势。

如果不同的工作组对各自的数据有所有权问题,那虚拟目录就是较好的选择,它不会改动数据,只是指向数据的位置而已。如果数据的准确性在整个企业内部更加重要,那元目录的方式当然更合适。

### 3. 从单点登录开始

建立起身份认证仓库并部署了管理工具之后,就可以开始部署使用数字身份认证技术的应用程序了。

SSO 是最常被引用的例子,它可以确保用户使用一个用户名和一个密码登录所有的应用程序。在 SSO 环境中,每个用户的身份认证,不再是一系列琐碎的用户名和密码,定义了他/她在网络上能做什么事情。因此,用户只需签到一次,即可得到相应应用程序和数据的访问权限。

在实际应用中,用户都非常喜欢 SSO 带来的操作过程的简化,但其实这并不是基于身份认证技术的最大好处。虽然一些 IT 管理员担心,一次登录就能够访问多个应用容易扩大攻击者对网络的破坏范围,但实际上当用户不得不维护多个用户名和密码时,他们更倾向于选择一些容易被猜出的密码,安全性反而容易受到威胁。如果是由 IT 部门指定的不易猜测的密码,用户则会把登录信息记录在纸上或是电子文档中,也很容易泄露密码。此外,用户要记的密码越多,就越有可能忘记其中的一两个,要是有几千用户,光是重新设置忘记的密码就会给 IT 支持部门造成很多不必要的工作量。而采用基于身份认证的单点登录技术,将能显著降低最终用户支持的成本。

### 4. 身份认证管理系统的其他优点

除了能实现 SSO,基于身份认证的网络管理还能帮助管理员集中创建和销毁网络账户。例如利用 Netegrity 公司 Identity Minder eProvision 产品等基于身份认证的配置(provisioning)系统,在几分钟内就可以为新雇员设置好电子邮件、应用程序和网络访问权限。其中许可权限可以基于已经建立好的规则进行分配,管理员只需要向系统输入一些简单信息,如员工姓名、职位、编号等,身份认证管理解决方案就能自动完成其余的配置工作。

与设立新账户相对应,从系统中删除账户也同样迅速。与在多个相互割裂的企业 IT 系统中手工删除所有信息(不能漏掉任何一个远程访问服务器、虚拟专用网、无线访问点等)相比,身份认证管理解决方案的自动化程度和准确程度显然更高,离职员工的密码被

遗漏在网络某个角落的风险大大降低。

Burton 集团的高级分析师 Mike Neuenschwander 表示，自动化配置能力将使大多数企业在身份认证管理上的投资得到快速而明显的回报。他还指出，作为身份认证管理系统中最具吸引力和最易部署的组件，自动化配置的市场非常诱人。

当然，自动化配置并不是一件简单的事情。除了为用户设置许可权限外，它还涉及到为移动设备、应用程序等授予权限，以及管理其他 IT 资产。此外，很多企业把它们的身份认证管理系统扩展到了企业网络之外，把合作伙伴、供应商、客户等都包含进来。

“就像飞机飞行不能只是依赖自动挡”，Neuenschwander 说道，“企业需要有专人负责策略设置、规则查看、进行必要的改动以及批准这些改动，最终对访问批准或拒绝负责的应该是企业的管理人员，而不是身份认证管理系统。”

## 7.3.7 802.1x 认证应用

目前，在实际实施的认证方式有 Web、PPPoE 和 802.1x 三种。Web 认证方式简单方便，但信息安全性很差，其兼容性和方便性是通过牺牲一定的安全性换来的。PPPoE 方式安全性较好，但设备投入较大。802.1x 安装设置比较麻烦，但拥有极好的信息安全性，可以和其他安全措施集成使用，便于构筑整体的网络安全体系。因此使用 802.1x 认证方式已经成为普遍采用的认证方式。

### 1. 802.1x 概述

802.1x 协议起源于 802.11 协议，后者是 IEEE 的无线局域网协议，制定 802.1x 协议的初衷是为了解决无线局域网用户的接入认证问题。IEEE 802 协议定义的局域网并不提供接入认证，只要用户能接入局域网控制设备(如 LAN Switch)，就可以访问局域网中的设备或资源。这在早期企业网有线 LAN 应用环境下并不存在明显的安全隐患。

随着移动办公及驻地网运营等应用的大规模发展，服务提供者需要对用户的接入进行控制和配置。尤其是 WLAN 的应用和 LAN 接入在电信网上大规模开展，有必要对端口加以控制以实现用户级的接入控制，802.1x 就是 IEEE 为了解决基于端口的接入控制(port-based network access control)而定义的一个标准。

### 2. 802.1x 认证体系

802.1x 是一种基于端口的认证协议，是一种对用户进行认证的方法和策略。端口可以是一个物理端口，也可以是一个逻辑端口(如 VLAN)。对于无线局域网来说，一个端口就是一个信道。802.1x 认证的最终目的就是确定一个端口是否可用。对于一个端口，如果认证成功，那么就“打开”这个端口，允许所有的报文通过。如果认证不成功，就使这个端口保持“关闭”，即只允许 802.1x 的认证协议报文通过。

802.1x 的体系结构如图 7-46 所示。它的体系结构中包括三个部分，即请求者系统、认证系统和认证服务器系统。

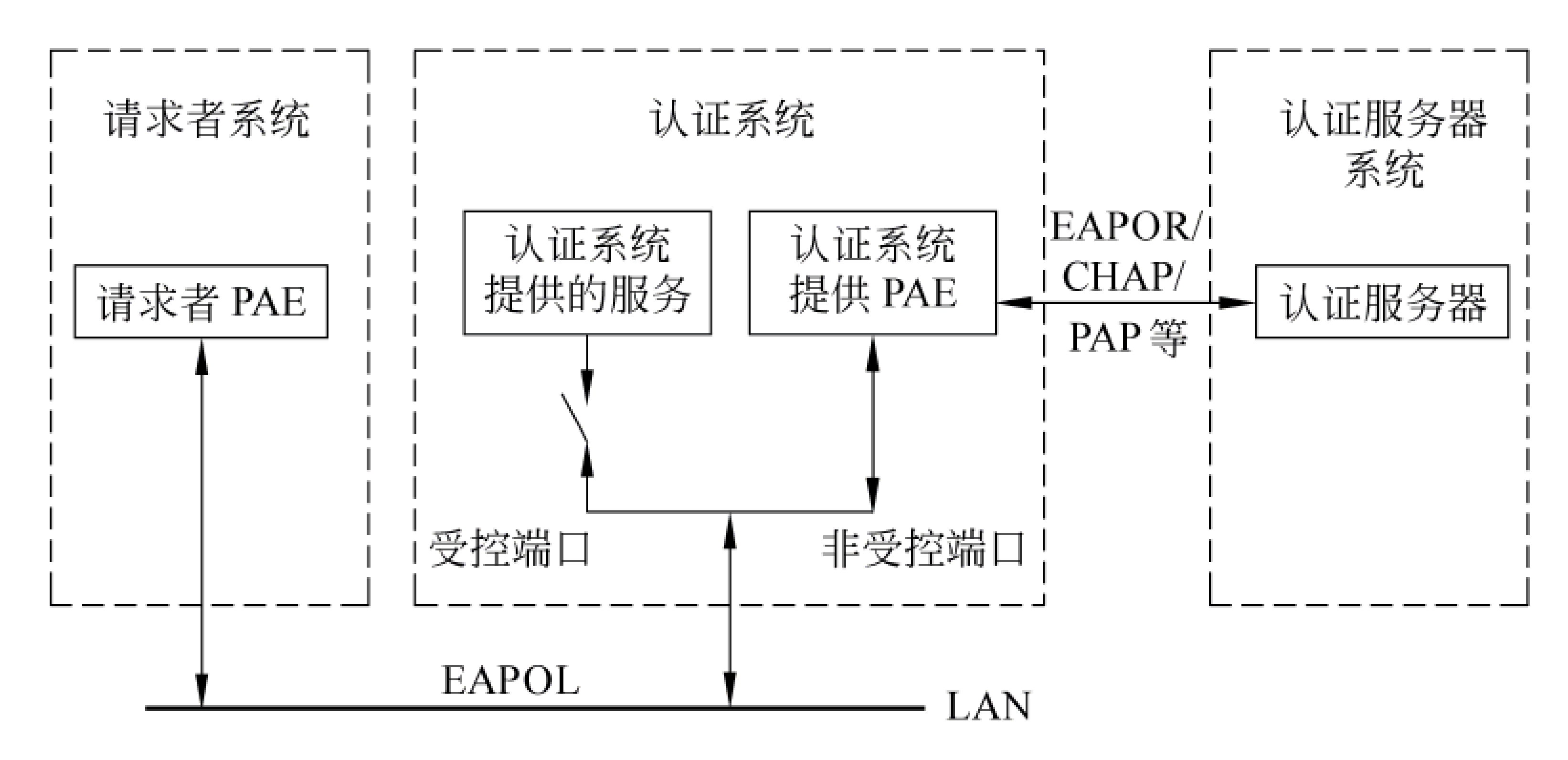



**图 7-46 IEEE 802.1x 认证的体系结构**

1）请求者系统

客户端系统一般为一个用户终端系统，该终端系统通常要安装一个客户端软件，用户通过启动这个客户端软件发起 IEEE 802.1x 协议的认证过程。为支持基于端口的接入控制，客户端系统需支持 EAPOL(extensible authentication protocol over LAN)协议。

2）认证系统

认证系统对连接到链路对端的认证请求者进行认证。认证系统通常为支持 IEEE 802.1x协议的网络设备。该设备对应于不同用户的端口(可以是物理端口，也可以是用户设备的 MAC 地址、VLAN、IP 等)有两个逻辑端口：受控(controlled port)端口和不受控端口(uncontrolled port)。不受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，可保证客户端始终可以发出或接受认证。受控端口只有在认证通过的状态下才打开，用于传递网络资源和服务。受控端口可配置为双向受控、仅输入受控两种方式，以适应不同的应用环境。如果用户未通过认证，则受控端口处于未认证状态，则用户无法访问认证系统提供的服务。一般在用户接入设备(如 LAN Switch 和 AP)上实现 802.1x 认证。

3）认证服务器系统

认证服务器存储有关用户的信息，例如用户所属的 VLAN、CAR 参数、优先级、用户的访问控制列表等。当用户通过认证后，认证服务器会把用户的相关信息传递给认证系统，由认证系统构建动态的访问控制列表，用户的后续流量就将接受上述参数的监管。认证服务器和 RADIUS 服务器之间通过 EAP 协议进行通信。建议使用 RADIUS 服务器来实现认证服务器的认证和授权功能。

请求者和认证系统之间运行 802.1x 定义的 EAPOL 协议。当认证系统工作于中继方式时，认证系统与认证服务器之间也运行 EAP 协议。EAP 帧中封装认证数据，将该协议承载在其他高层次协议中(如 RADIUS)，以便穿越复杂的网络到达认证服务器。当认证系统工作于终结方式时，认证系统终结 EAPOL 消息，并转换为其他认证协议(如 RADIUS)，传递用户认证信息给认证服务器系统。

认证系统每个物理端口内部包含有受控端口和非受控端口。非受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，可随时保证接收认证请求者发出的 EAPOL 认证报文。受控端口只有在认证通过的状态下才打开，用于传递网络资源和服务。

### 3. 和其他认证方式的比较

IEEE 802.1x 协议虽然源于 IEEE 802.11 无线以太网(EAPOW),但是,它在以太网中的引入,解决了传统的 PPPoE 和 Web/Portal 认证方式带来的问题,消除了网络瓶颈,减轻了网络封装开销,降低了建网成本。

众所周知,PPPoE 是从基于 ATM 的窄带网引入到宽带以太网的,由此可以看出,PPPoE 并不是为宽带以太网量身订做的认证技术,将其应用于宽带以太网,必然会有其局限性。虽然其方式较灵活,在窄带网中有较丰富的应用经验,但是它的封装方式,也造成了宽带以太网的种种问题。在 PPPoE 认证中,认证系统必须将每个包进行拆解才能判断和识别用户是否合法,一旦用户增多或者数据包增大,封装速度必然跟不上,成为了网络瓶颈。其次这样大量的拆包解包过程必须由一个功能强劲同时价格昂贵的设备来完成,这个设备就是传统的 BAS。对于每个用户发出的每个数据包,BAS 必须进行拆包识别和封装转发。为了解决瓶颈问题,厂商想出了提高 BAS 性能,或者采用大量分布式 BAS 等方式来解决问题,但是 BAS 的功能就决定了它是一个昂贵的设备,这样一来建设成本就会越来越高。

Web/Portal 认证是基于业务类型的认证,不需要安装其他客户端软件,只需要浏览器就能完成,就用户来说较为方便。但是由于 Web 认证是 7 层协议,从逻辑上来说为了达到网络 2 层的连接而跑到 7 层做认证,这首先不符合网络逻辑。其次由于认证是 7 层协议,对设备必然提出更高要求,增加了建网成本。第三,Web 是在认证前就为用户分配了 IP 地址,对目前网络珍贵的 IP 地址来说造成了浪费,而且分配 IP 地址的 DHCP 服务器对用户而言是完全裸露的,容易造成被恶意攻击,一旦受攻击瘫痪,整网就没法认证。为了解决易受攻击问题,就必须加装一个防火墙,这样一来又大大增加了建网成本。Web/Portal 认证用户连接性差,不容易检测用户离线,基于时间的计费较难实现。用户在访问网络前,不管是 Telnet、FTP 还是其他业务,必须使用浏览器进行 Web 认证,易用性不够好,而且认证前后业务流和数据流无法区分。所以在以太网中,Web/Portal 认证目前只是限于在酒店等特殊网络环境中使用。Web、PPPoE 和 802.1x 认证的区别参见表 7-1。

**表 7-1 三种认证方式的比较**

| | Web | PPPoE | 802.1x |
|---|---|---|---|
| 客户端软件 | 不需要 | 需要 | 需要 |
| 安装设置 | 不需要 | 需要 | 需要 |
| 标准程度 | 厂家私有 | RFC2516 | IEEE 标准 |
| 封装开销 | 小 | 较大 | 小 |
| 接入控制方式 | 用户 | 用户 | 端口 |
| IP 地址 | 认证前分配 | 认证后分配 | 认证后分配 |
| VLAN 数目要求 | 多 | 无 | 无 |
| 设备支持 | 厂家私有 | 业界设备 | 业界设备 |

### 4. 802.1x 协议技术优点

IEEE 802.1x 协议为二层协议，不需要到达三层，协议实现简单，对设备的整体性能要求不高，可以有效降低建网成本。同时 IEEE 802.1x 的认证体系结构中采用了“可控端口”和“不可控端口”的逻辑功能，从而可以实现业务与认证的分离。用户通过认证后，业务流和认证流实现分离，对后续的数据包处理没有特殊要求，业务可以很灵活，尤其在开展宽带组播等方面的业务有很大的优势，所有业务都不受认证方式限制。

总结起来，802.1x 认证具有以下优点。

(1) 简洁高效：纯以太网技术内核，保持 IP 网络无连接特性，去除冗余昂贵的多业务网关设备，消除网络认证计费瓶颈和单点故障，易于支持多业务。

(2) 容易实现：可在普通 L3、L2、IP DSLAM 上实现，网络综合造价成本低。

(3) 安全可靠：在二层网络上实现用户认证，结合 MAC、端口、账户和密码等。绑定技术具有很高的安全性。

(4) 行业标准：IEEE 标准，微软操作系统内置支持。

(5) 易于运营：控制流和业务流完全分离，易于实现多业务运营，少量改造传统包月制等单一收费制网络即可升级成运营级网络。

### 5. 802.1x 认证流程

基于 802.1x 的认证系统在客户端和认证系统之间使用 EAPOL 格式封装 EAP 协议传送认证信息，认证系统与认证服务器之间通过 RADIUS 协议传送认证信息。由于 EAP 协议的可扩展性，基于 EAP 协议的认证系统可以使用多种不同的认证算法，如 EAP-MD5、EAP-TLS、EAP-SIM、EAP-TTLS 以及 EAP-AKA 等认证方法。

以 EAP-MD5 为例，描述 802.1x 的认证流程。EAP-MD5 是一种单向认证机制，可以完成网络对用户的认证，但认证过程不支持加密密钥的生成。基于 EAP-MD5 的 802.1x认证系统功能实体协议栈如图 7-47 所示，基于 EAP-MD5 的 802.1x 认证流程如图 7-48 所示。

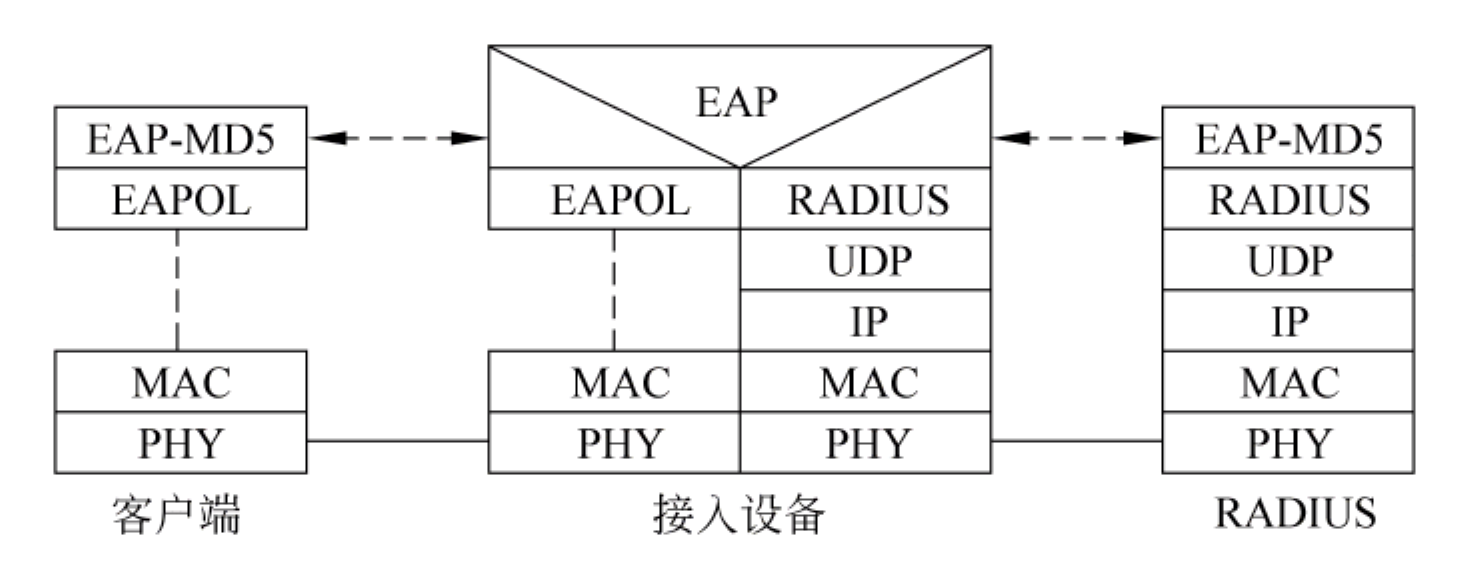



**图 7-47　基于 EAP-MD5 的 802.1x 认证系统功能实体协议栈**

认证流程包括以下步骤。

(1) 客户端向接入设备发送一个 EAPOL-Start 报文，开始 802.1x 认证接入。

(2) 接入设备向客户端发送 EAP-Request/Identity 报文，要求客户端将用户名送上来。

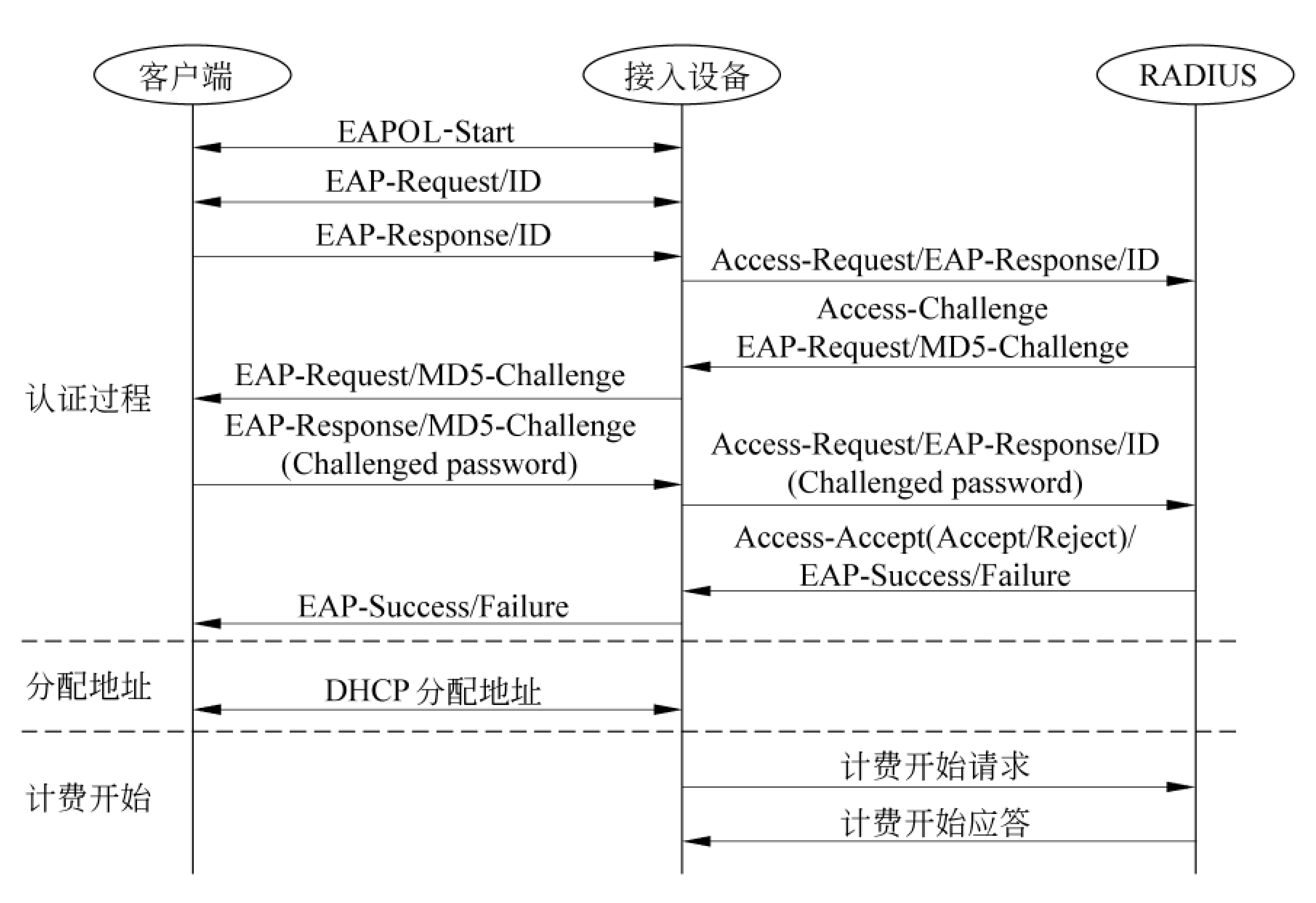



**图 7-48 基于 EAP-MD5 的 802.1x 认证流程**

(3) 客户端回应一个 EAP-Response/Identity 给接入设备的请求，其中包括用户名。

(4) 接入设备将 EAP-Response/Identity 报文封装到 RADIUS Access-Request 报文中，发送给认证服务器。

(5) 认证服务器产生一个 Challenge，通过接入设备将 RADIUS Access-Challenge 报文发送给客户端，其中包含有 EAP-Request/MD5-Challenge。

(6) 接入设备通过 EAP-Request/MD5-Challenge 发送给客户端，要求客户端进行认证。

(7) 客户端收到 EAP-Request/MD5-Challenge 报文后，将密码和 Challenge 做 MD5 算法后的 Challenged-password，在 EAP-Response/MD5-Challenge 回应给接入设备。

(8) 接入设备将 Challenge、Challenged password 和用户名一起送到 RADIUS 服务器，由 RADIUS 服务器进行认证。

(9) RADIUS 服务器根据用户信息，做 MD5 算法，判断用户是否合法，然后回应认证成功/失败报文到接入设备。如果成功，携带协商参数以及用户的相关业务属性给用户授权。如果认证失败，则流程到此结束。

(10) 如果认证通过，用户通过标准的 DHCP 协议(可以是 DHCP Relay)，通过接入设备获取规划的 IP 地址。

(11) 接入设备发起计费开始请求给 RADIUS 用户认证服务器。

(12) RADIUS 用户认证服务器回应计费开始请求报文，用户上线完毕。

**6. 802.1x 认证组网应用**

按照不同的组网方式，802.1x 认证可以采用集中式组网(汇聚层设备集中认证)、分布式组网(接入层设备分布认证)和本地认证组网。不同的组网方式下，802.1x 认证系统

实现的网络位置有所不同。

1）802.1x 集中式组网（汇聚层设备集中认证）

802.1x 集中式组网方式是将 802.1x 认证系统端放到网络位置较高的 LAN Switch 设备上，这些 LAN Switch 为汇聚层设备。其下挂的网络位置较低的 LAN Switch 只将认证报文透传给作为 802.1x 认证系统端的网络位置较高的 LAN Switch 设备，集中在该设备上进行 802.1x 认证处理。这种组网方式的优点在于 802.1x 采用集中管理方式，降低了管理和维护成本。汇聚层设备集中认证如图 7-49 所示。

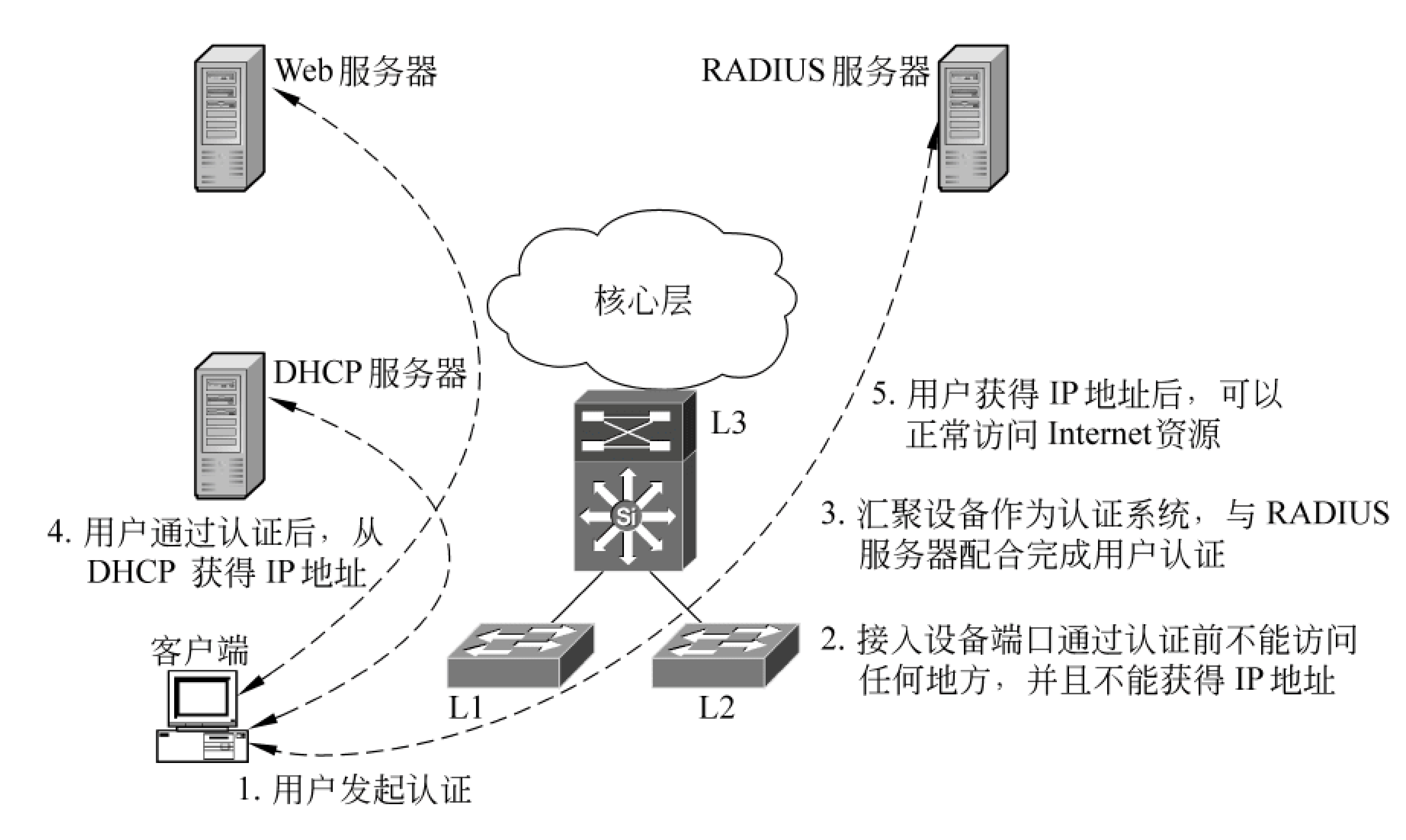



图 7-49 IEEE802.1x 集中式组网（汇聚层设备集中认证）

2）802.1x 分布式组网（接入层设备分布认证）Relay

802.1x 分布式组网是把 802.1x 认证系统端放在网络位置较低的多个 LAN Switch 设备上，这些 LAN Switch 作为接入层边缘设备。认证报文送给边缘设备，进行 802.1x 认证处理。这种组网方式的优点在于，它采用中/高端设备与低端设备认证相结合的方式，可满足复杂网络环境的认证。认证任务分配到众多的设备上，减轻了中心设备的负荷。接入层设备分布认证如图 7-50 所示。

802.1x 分布式组网方式非常适用于受控组播等特性的应用，建议采用分布式组网对受控组播业务进行认证。如果采用集中式组网将受控组播认证设备端放在汇聚设备上，从组播服务器下行的流在到达汇聚设备之后，由于认证系统还下挂接入层设备，将无法区分最终用户。若打开该受控端口，则汇聚层端口以下的所有用户都能够访问到受控组播消息源。反之，如果采用分布式组网，则从组播服务器来的组播流到达接入层认证系统，可以实现组播成员的精确粒度控制。

3）802.1x 本地认证组网

802.1x 的 AAA 认证可以在本地进行，而不用到远端认证服务器上去认证。这种本地认证的组网方式在专线用户或小规模应用环境中非常适用。它的优点在于节约成本，不需要单独购置昂贵的服务器，但随着用户数目的增加，还需要由本地认证向 RADIUS 认证迁移。

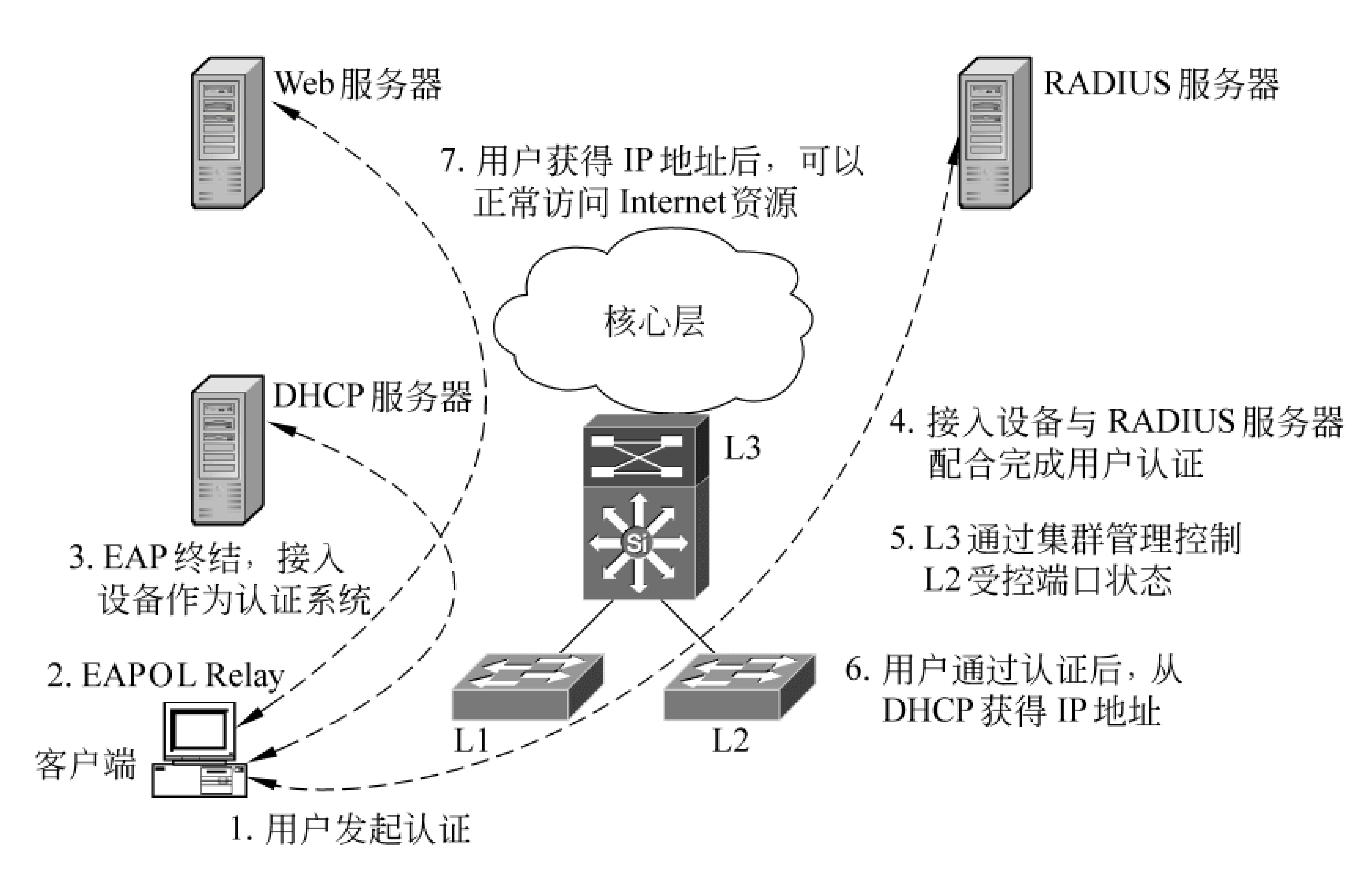



**图 7-50 IEEE 802.1x 分布式组网(接入层设备分布认证)**

802.1x 认证系统提供了一种用户接入认证的手段，它仅关注端口的打开与关闭。对于合法用户(根据账号和密码)接入时，该端口打开，而对于非法用户接入或没有用户接入时，则使端口处于关闭状态。认证的结果在于端口状态的改变，而不涉及其他认证技术所考虑的 IP 地址协商和分配问题，是各种认证技术中最为简化的实现方案。

必须注意到 802.1x 认证技术的操作颗粒度为端口，合法用户接入端口之后，端口始终处于打开状态，此时其他用户(合法或非法)通过该端口接入时，不需认证即可访问网络资源。如果需要更高级别的安全，还需要和访问控制结合进行认证。对于无线局域网接入而言，认证之后建立起来的信道(端口)被独占，不存在其他用户非法使用的问题。

# 7.4 虚拟专网

## 7.4.1 虚拟专网概述

### 1. 虚拟专网基本原理

虚拟专网是虚拟私有网络，它是一种利用公共网络来构建的私有专用网络。目前，能够用于构建 VPN 的公共网络包括 Internet 和服务提供商(ISP)所提供的 DDN 专线(data digit network leased lind)、帧中继(frame relay)、ATM 等，构建在这些公共网络上的 VPN 将给企业提供集安全性、可靠性和可管理性于一身的私有专用网络。

“虚拟”的概念是相对传统私有专用网络的构建方式而言的，对于广域网连接，传统的组网方式是通过远程拨号和专线连接来实现的，而 VPN 是利用服务提供商所提供的公共网络来实现远程的广域连接。通过 VPN(模型如图 7-51 所示)，企业可以以明显更低的成本连接它们的远地办事机构、出差工作人员以及业务合作伙伴。

为了形成这样的链路，采用了所谓的“隧道”技术。可以模仿点对点连接技术，依靠

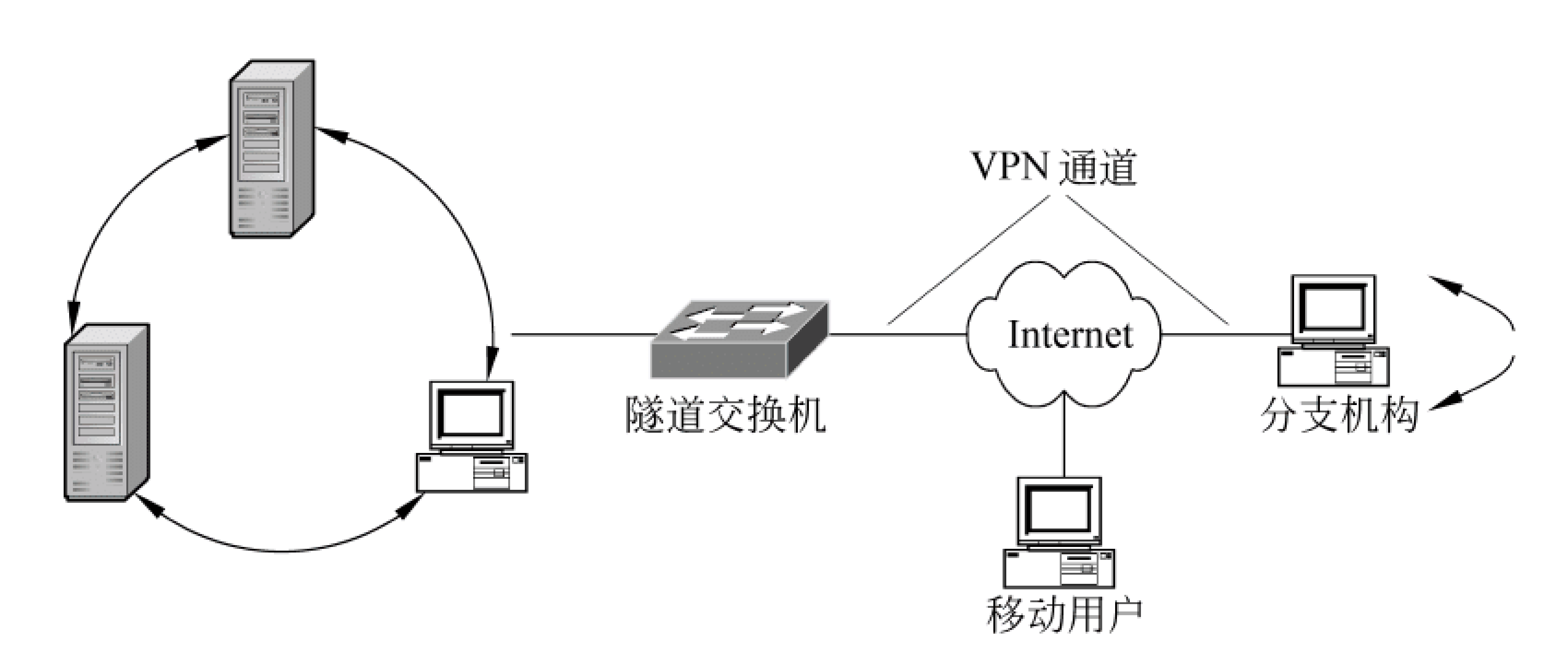



**图 7-51 VPN 模型**

Internet 服务提供商(ISP)和其他的网络服务提供商(NSP)在公用网中建立自己专用的"隧道",让数据包通过这条隧道传输加密传输专用数据流量。在 VPN 中,PPP 数据包流是由一个 LAN 上的路由器发出,通过共享 IP 网络上的隧道进行传输,再到达另一个 LAN 上的路由器。隧道代替了实实在在的专用线路。对于不同的信息来源,可分别给它们开出不同的隧道。于是,兼容性问题、不同的服务质量要求以及其他的麻烦都迎刃而解。

虚拟网络用户在安全性可得到完全保证的前提下,均可通过当地的电话或租用线路服务建立联系,而不必租用长途线路,连接各机构的所有办公室、远程工作人员、移动员工,甚至于国内外范围的客户和供应商。虚拟专网减少了设备需求及网络维护责任,能够为用户节省大量的开支。

然而选择一个合适的 VPN 解决方案或产品对一个管理人员来说是困难的,因为每一种解决方案都可提供不同程度的安全性、可用性,并且都各有优缺点。为了选择一个合适的 VPN 产品,决策者应该首先明确他们公司的商业需求,例如公司是需要将少数几个可信的远地雇员联到公司总部,还是希望为每个分支机构合作伙伴、供应商、顾客和远地雇员都建立一个安全连接通道。不管怎样,一个 VPN 至少应该能提供如下功能。

(1) 加密数据以保证通过公网传输的信息即使被他人截获也不会泄露。

(2) 信息认证和身份认证保证信息的完整性、合法性并能鉴别用户的身份。

(3) 提供访问控制,不同的用户有不同的访问权限。

基于 Internet 建立的 VPN 如果实施得当,可以保护网络免受病毒感染、防止欺骗、防止商业间谍、增强访问控制、增强系统管理及加强认证等。在 VPN 提供的功能中,认证和加密是最重要的。而访问控制相对比较复杂,因为它的配置与实施策略和所用工具紧密相关。VPN 的三种功能必须相互配合才能保证真正的安全性。

目前,VPN 技术已经成为防火墙的重要功能,绝大多数防火墙都支持 VPN,因此利用防火墙构建 VPN 已经成为一种经典的方案,这样既可以发挥防火墙本身的功能,又可以允许远程用户通过防火墙联入一个内部网络。

### 2. VPN 的优点

1) 降低成本

借助 ISP 来建立 VPN,对于 VPN 用户而言,利用 Internet 组建私有网,将大笔的专

线费用缩减为少量的市话费用和 Internet 费用，就可以节省大量的通信费用。此外，VPN 还使企业不必投入大量的人力和物力去安装和维护 WAN 设备和远程访问设备。这些工作都由 ISP 负责完成。

2）容易扩展

如果想扩大 VPN 的容量和覆盖范围。总部需要做的事情很少，而且能立即实现。企业只需与新的 ISP 签约，建立账户或者与原有的 ISP 重签合约，扩大服务范围。在远程办公室增加 VPN 能力也很简单。通过配置命令就可以使 Extranet 路由器拥有 Internet 和 VPN 能力，路由器还能对工作站自动进行配置。

3）可随意与合作伙伴联网

如果想与合作伙伴联网，没有 VPN，双方的信息技术部门就必须协商如何在双方之间建立租用线路或帧中继线路。有了 VPN 之后，这种协商就毫无必要，真正达到了要连就连、要断就断。

4）完全控制主动权

VPN 使用户可以利用 ISP 的设施和服务，同时又完全掌握着自己网络的控制权。比方说，VPN 用户的网络地址可以由企业内部进行统一分配、VPN 组网的灵活方便等特性将大大方便企业的网络管理；用户可以把拨号访问交给 ISP 去做，由自己负责用户的查验、访问权、网络地址、安全性和网络变化管理等重要工作。另外，在 VPN 应用中，通过远端用户认证以及隧道数据加密等技术使得通过公用网络传输的私有数据的安全性得到了很好的保证。

### 7.4.2 VPN 相关技术

对于构建 VPN 来说，网络隧道（tunnelling）技术是个关键技术，它主要利用网络隧道协议来实现两个网络协议之间的传输。网络隧道技术涉及了三种网络协议，有网络隧道协议、隧道协议下面的承载协议和隧道协议所承载的被承载协议。现有两种类型的隧道协议，一种是二层隧道协议，用于传输二层网络协议，它主要应用于构建 Access VPN；另一种是三层隧道协议，用于传输三层网络协议，它主要应用于构建 Intranet VPN 和 Extranet VPN。

#### 1. 二层隧道协议

二层隧道协议主要有三种，分别是微软、Ascend、3COM 等公司支持的点对点隧道协议（point to point tunneling protocol，PPTP），Windows NT 4.0 以上版本中有支持。Cisco、北方电信等公司支持的二层转发协议（layer 2 forwarding，L2F），在 Cisco 路由器中有支持。而由 IETF 起草，微软 Ascend、Cisco、3COM 等公司参与的二层隧道协议（layer 2 tunneling protocol，L2TP）结合了上述两个协议的优点，将很快地成为 IETF 有关二层隧道协议的工业标准。

#### 2. 三层隧道协议

用于传输三层网络协议的隧道协议叫三层隧道协议。三层隧道协议并非是一种很

新的技术，早已出现的 RFC 1701（generic routing encapsulation，GRE）协议就是个三层隧道协议。新出来的 IETF 的 IP 层加密标准协议 IPSec 协议也是个三层隧道协议。IPSec 协议不是一个单独的协议，它给出了应用于 IP 层上网络数据安全的一整套体系结构，它包括网络安全协议（authentication header，AH）和（encapsulating security payload，ESP）协议、密钥管理协议（internet key exchange，IKE）协议和用于网络认证及加密的一些算法等。IPSec 规定了如何在对等层之间选择安全协议、确定安全算法和密钥交换，向上提供了访问控制、数据源认证、数据加密等网络安全服务。

**3. 安全技术**

在公用网络上构建 VPN 传输私有数据，网络安全性是个很重要的问题。在 VPN 应用中应用了一系列的网络安全技术，如网络防火墙、应用 IPSec 进行隧道上的网络数据加密、进行 L2TP 隧道端的相互认证等，使得在公用网络上传输的私有网络数据的安全性得到了保证。

安全性通过以下几个方面来得到保证。

（1）在 VPN 用户拨入 LAC（接入服务器）时，即使被发现是 VPN 用户（比如通过用户名中的域名），仍需要与接入服务器端的 RADIUS 服务器进行用户身份认证。如果认证不通过，则用户不能使用 VPN 业务。

（2）在建立 L2TP 隧道时，通道两端需要相互认证，LNS 端对于 VPN 用户可以再次进行身份认证。

（3）在 VPN 用户通过接入服务器端的身份认证时，将和普通用户类似受权限限制，不能任意访问网内资源。

（4）最终接入内部网认证由用户实现，在这种情况下，需要有自己的认证服务器。

### 7.4.3 VPN的分类及用途

在连接到 Internet 之前，用户应制定出相应的安全策略，清楚地说明不同身份的用户可以访问哪些资源。一个更安全的解决方案可能包括防火墙、路由器、代理服务器、VPN 软件或硬件。它们中的任何一种设备可能提供足够的安全通信，但是采用何种设备取决于用户的安全策略。

根据不同需要可以构造不同类型的 VPN，不同商业环境对 VPN 的要求和 VPN 所起的作用是不一样的。下面分三种情况说明 VPN 的用途。

**1. 企业内部虚拟专网（Intranet VPN）**

在公司总部和它的分支机构之间建立 VPN，称为内部网 VPN。内部网是通过公共网络将某一个用户的各分支机构的 LAN 连接而成的网络。这种类型的 LAN 到 LAN 的连接带来的风险最小，因为用户通常认为他们的分支机构是可信的，这种方式连接而成的网络被称为 Intranet，可把它作为公司网络的扩展。

当一个数据传输通道的两个端点被认为是可信的时候，用户可以选择“内部 VPN”解决方案，安全性主要在于加强两个 VPN 服务器之间加密和认证的手段，如图 7-52 所示。

大量的数据经常需要通过 VPN 在局域网之间传递，把中心数据库或其他计算资源连接起来的各个局域网可以看成是内部网的一部分。

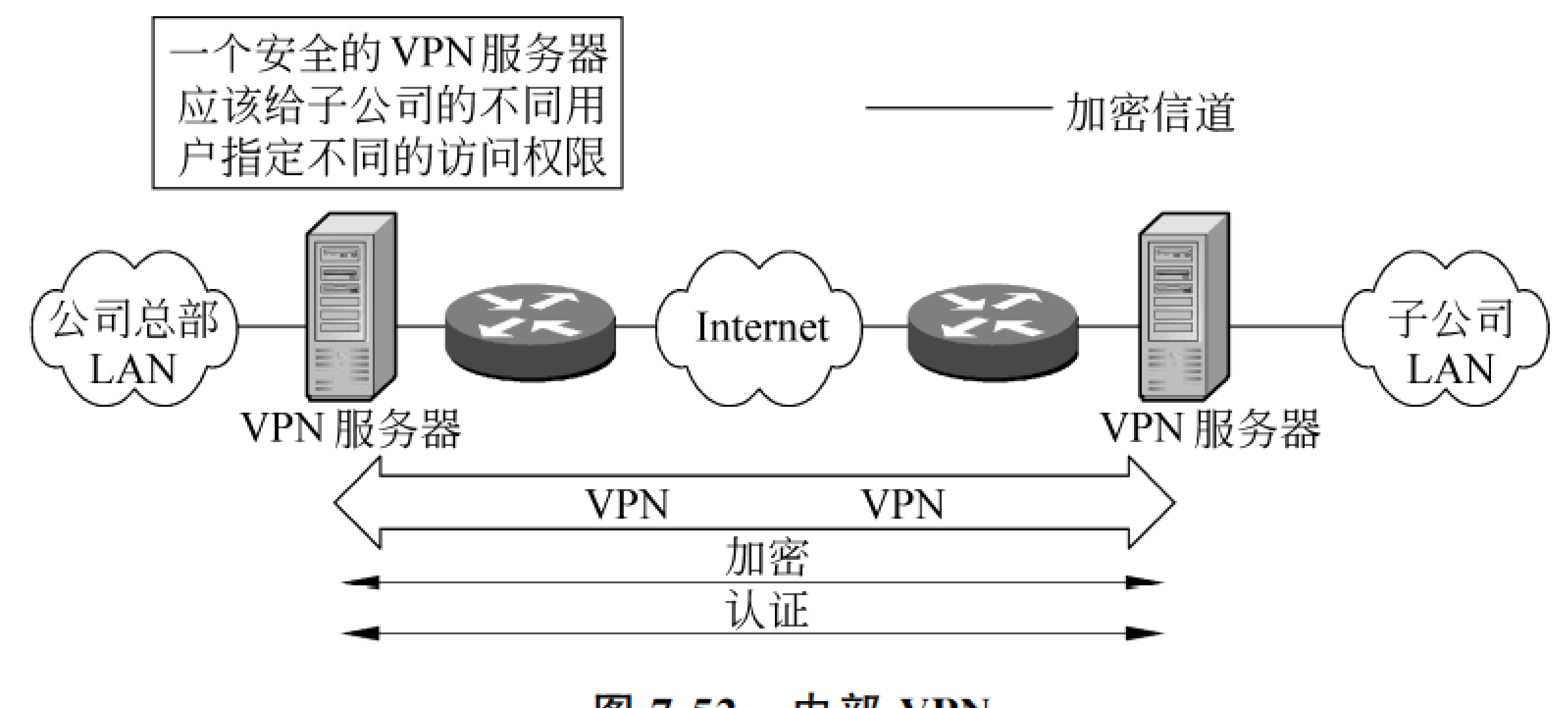



图 7-52 内部 VPN

这里仅是用户的分支机构中有一定访问权限的用户才能通过“内部网 VPN”访问用户总部的资源，所有端点之间的数据传输都要经过加密和身份鉴别。如果一个用户对其分支机构或个人有不同的可信程度，那么用户可以考虑基于认证的 VPN 方案来保证信息的安全传输而不是靠可信的通信子网。

这种类型的 VPN 主要任务是保护用户的 Intranet 不被外部入侵，同时保证用户的重要数据流经 Internet 时的安全性。

**2. 访问虚拟专网（access VPN）**

在用户内部和远地雇员或旅行之中的雇员之间建立 VPN，称为访问 VPN。现在，人们意识到通过 Internet 的远程拨号访问所带来的好处。用 Internet 作为远程访问的骨干网比传统的方案更容易实现，而且花钱更少。如果一个用户无论是在家里还是在旅途之中，他想同自己的内部网建立一个安全连接，则可以用访问 VPN 来实现，如图 7-53 所示。典型的访问 VPN 是用户通过本地的 Internet 服务提供商（ISP）登录到 Internet 上，并在现在的办公室和用户内部网之间建立一条加密信道。访问 VPN 的客户端应尽量简单，因为普通雇员一般都缺乏专门训练。客户应可以手工建立一条 VPN 信道，即当客户每次想建立一个安全通信信道时，只需安装 VPN 软件。在服务器端，因为要监视大量用户，有时需要增加或删除用户，这样可能造成混乱，并带来风险，因此服务器应集中并且管理要容易。

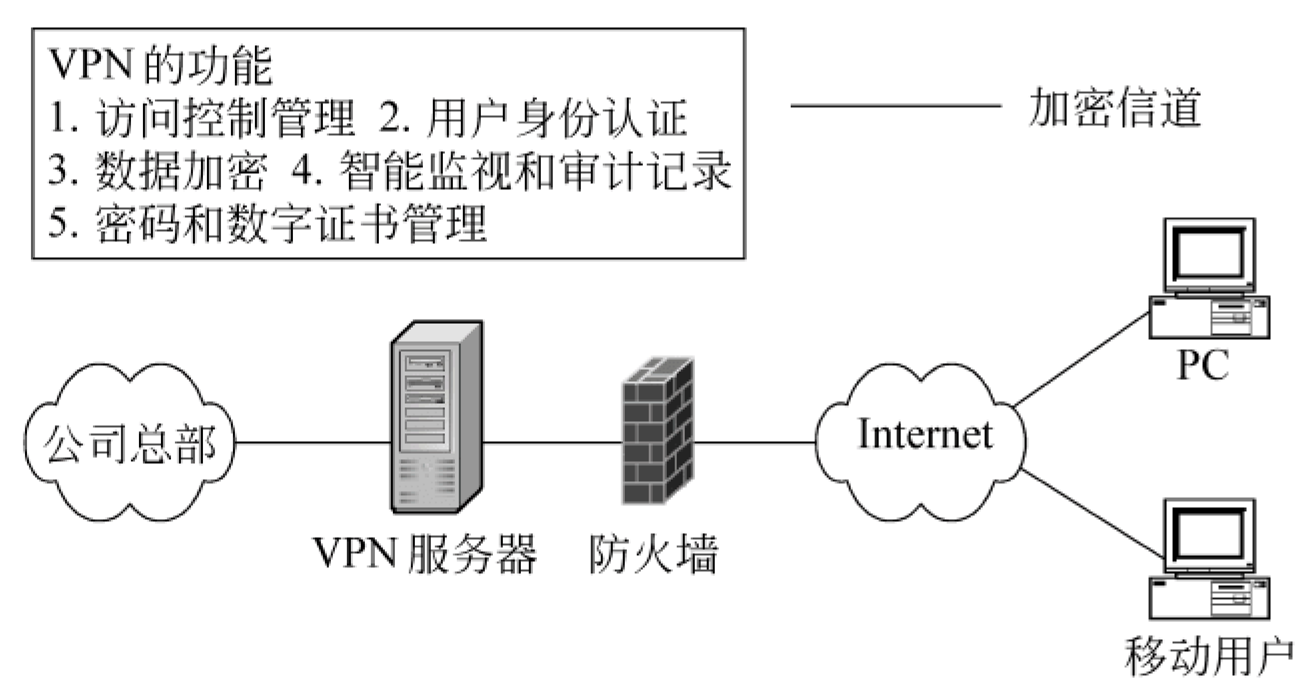



图 7-53 访问 VPN

用户往往指定一种"透明的访问策略",即使在远处的雇员也能像他们坐在用户总部的办公室一样自由地访问用户的资源。因此首先要考虑的是所有端到端的数据都要加密,并且只有特定的接收者才能解密。大多数 VPN 除了加密以外还要考虑加密密码的强度和认证方法。这种 VPN 要对个人用户的身份进行认证,而不仅认证地址,这样用户总部就会知道哪个雇员欲访问用户的内部网络,认证后决定是否允许用户对网络资源的访问。认证技术可以包括用一次密码、Kerberos 认证方案、令牌卡、智能卡或者指纹。一旦一个用户同 VPN 服务器进行了认证,根据他的访问权限表,他就有一定程度的访问权限。每个人的访问权限表由网络管理员制定,并且符合公司的安全策略。

有较高安全度的远程访问 VPN 应能截取到特定主机的信息流,有加密、身份认证和过滤等功能。

### 3. 扩展企业内部虚拟专网(extranet VPN)

在用户与商业伙伴、顾客、供应商和投资者之间建立的 VPN,称为扩展企业内部 VPN。扩展企业内部 VPN 为用户合作伙伴、顾客、供应商和在异地的用户雇员提供安全性,如图 7-54 所示。它应能保证包括 TCP 和 UDP 服务在内的各种应用服务的安全,如 E-mail、HTTP、FTP、RealAudio 和数据库以及一些应用程序,如 Java 与 ActiveX 的安全。因为不同用户的网络环境是不同的,一个可行的扩展企业内部 VPN 方案应能适用于各种操作平台、协议、各种不同的认证方案和加密算法。

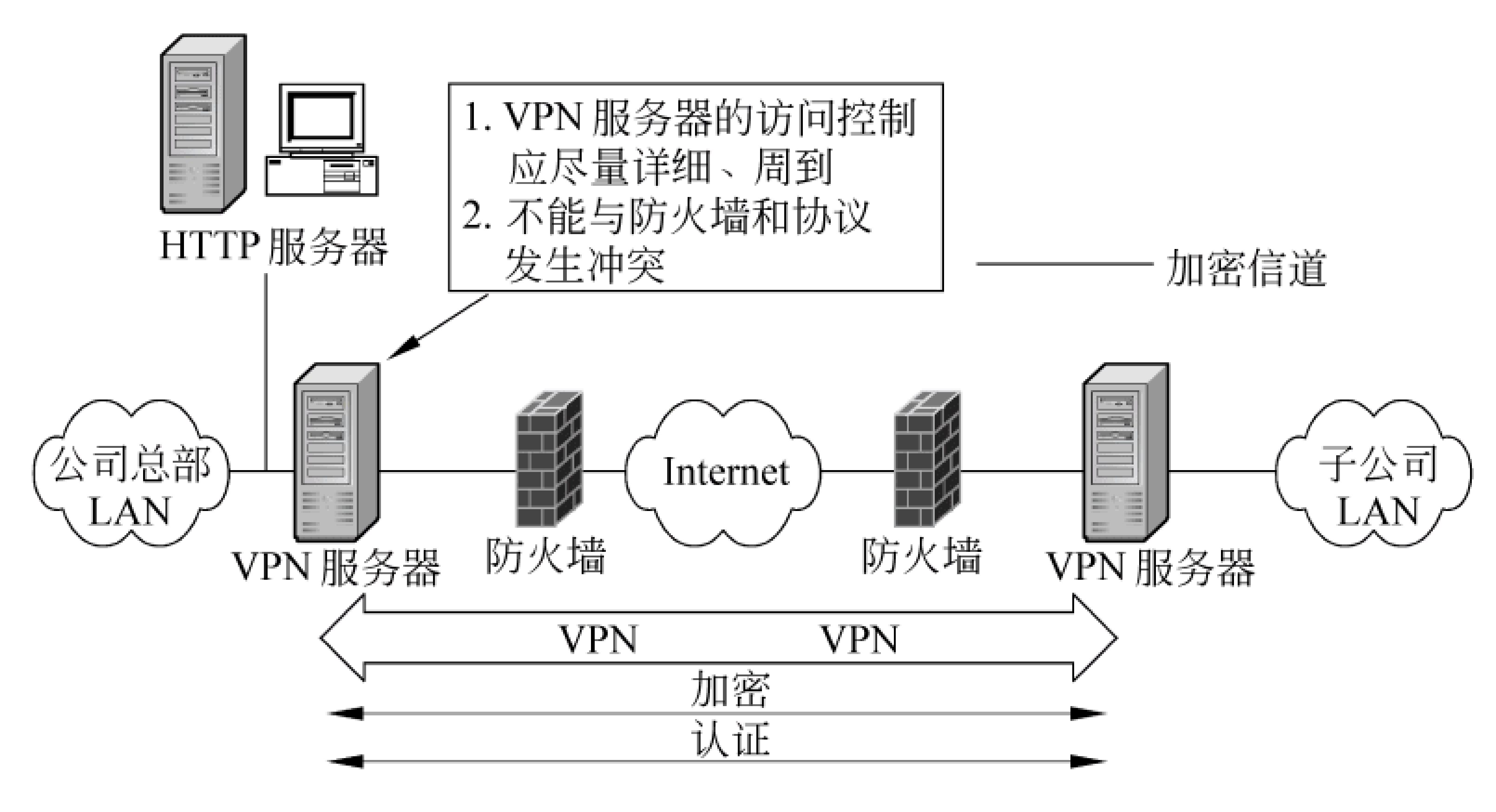



**图 7-54 扩展企业内部 VPN**

扩展企业内部 VPN 的主要目标是保证数据在传输过程中不被修改,保护网络资源不受外部威胁。安全的扩展企业内部 VPN 要求用户在同它的顾客、合作伙伴及在外地的雇员之间经 Internet 建立端到端的连接时,必须通过 VPN 服务器才能进行在这种系统上,网络管理员可以为合作伙伴的职员指定特定的许可权,例如可以允许对方的销售经理访问一个受到保护的服务器上的销售报告。

扩展企业内部 VPN 中应是一个由加密、认证和访问控制功能组成的集成系统。通常用户将 VPN 代理服务器放在一个不能穿透的防火墙隔离层之后,防火墙阻止所有来历不明的信息传输。所有经过过滤后的数据通过一个唯一的入口传到 VPN 服务器,

VPN 服务器再根据安全策略来进一步过滤。

VPN 可以建立在网络协议的上层，如应用层，也可建立在较低的层次，如网络层。在应用层的 VPN 可以用一个代理服务器实现，这就是说，不直接打开任何到公司内部网的连接，这样有了 VPN 代理服务器之后，就可以防止 IP 地址欺骗。所有的访问都要经过代理，这样管理员就可以知道谁企图访问内部网以及他做了多少次这种尝试。

扩展企业内部 VPN 并不假定连接的用户双方之间存在双向信任关系。扩展企业内部 VPN 在 Internet 内打开一条隧道，并保证经数据包过滤后信息传输的安全。当用户将很多商业活动都通过公共网络进行交易时，一个扩展企业内部 VPN 应该用高强度的加密算法密钥应选在 128bits 以上。此外，应支持多种认证方案和加密算法，因为商业伙伴和顾客可能有不同的网络结构和操作平台。

扩展企业内部 VPN 应能根据尽可能多的参数来控制对网络资源的访问参数，包括源地址、目的地址、应用程序的用途所用的加密和认证类型、个人身份、工作组及子网等。管理员应能对个人进行身份认证，而不仅仅根据 IP 地址来进行身份认证。

## 7.4.4 VPN 解决方案

### 1. 解决方案 1——由用户端建立的拨号 VPN

首先，远程客户拨号进入一个本地接入点(POP)，然后运行一个支持 IPSec 的客户端软件，与客户内联网中的一台 PIX 防火墙建立一条加密的隧道，这样就可以安全地访问防火墙内的主机了。

该方案的优点是访问服务器不参与 VPN，客户可以同时访问互联网和内联网。缺点是客户端软件必须是指定的支持 IPSec 的产品；隧道对于 ISP 是完全透明的，用户无法得到 ISP 的增值服务；IP 地址由 ISP 分配，不能采用内部地址。

### 2. 解决方案 2——由访问服务器建立的拨号 IP-VPN

采用防火墙通过 L2F 或 L2TP 协议，由防火墙建立一条安全隧道的内联网网关，该网关负责身份认证和 IP 地址分配，远程客户就像直接联到内联网一样。

该方案的优点是远程用户端不需要特别的软件；ISP 可以提供高档次的拨号 IP-VPN 服务；IP 地址可以采用的内联网的内部地址，不占用 ISP 的地址空间。缺点是不适合在国际互联网上采用。

### 3. 解决方案 3——IPSec IP 隧道的专线 VPN

任何一台支持 IPSec 的设备之间都可以建立一条加密隧道，支持 IPSec 的设备包括运行 IPSec 软件的客户机、路由器、防火墙和服务器。

该方案的优点是方便、快捷，无须改变 ISP 的网络；安全、可靠、性能高；ISP 可以对隧道提供高级的 IP 服务。

#### 4. 解决方案 4——GRE 隧道的专线 VPN

GRE 隧道是基于 RFC 1701 和 RFC 1702 的标准 VPN 方案。它的做法是将 IP 数据包加上 GRE 头，封装在 IP 数据包内。在路由器看来 GRE 隧道是一个点到点端口，它可以被加密。ISP 可以对 GRE 隧道提供 QoS 服务，但这个隧道的两端必须在同一个 ISP 的网络内。推荐用户采用此方式。

该方案的优点是用户自己定义内部的 IP 地址；ISP 可以提供针对应用层的 IP QoS 服务；与媒体无关。缺点是只能在一个 ISP 网络内。

#### 5. 解决方案 5——基于 MPLS 的内嵌 VPN 网络

在整个网络上运行 MPLS，每一个 VPN 都有一个 VPN-ID，通过 TCP 将不同的 VPN-ID 映射到不同的 TAG 上，这样 VPN 的信息就内嵌在 MPLS 网络中。

该方案的优点是 TAG-VPN 是无连接的，无须定义隧道；与 MPLS 一样具有良好的网络扩展性和增值服务扩展性；在 ISP 网络中可以“看见”VPN，可以为每个 VPN 提供增值服务；容易增加 VPN 和简化管理；IP QoS 和流量管理随 MPLS 与生具有。缺点是需要高端路由器。

VPN 解决方案模型如图 7-55 所示。

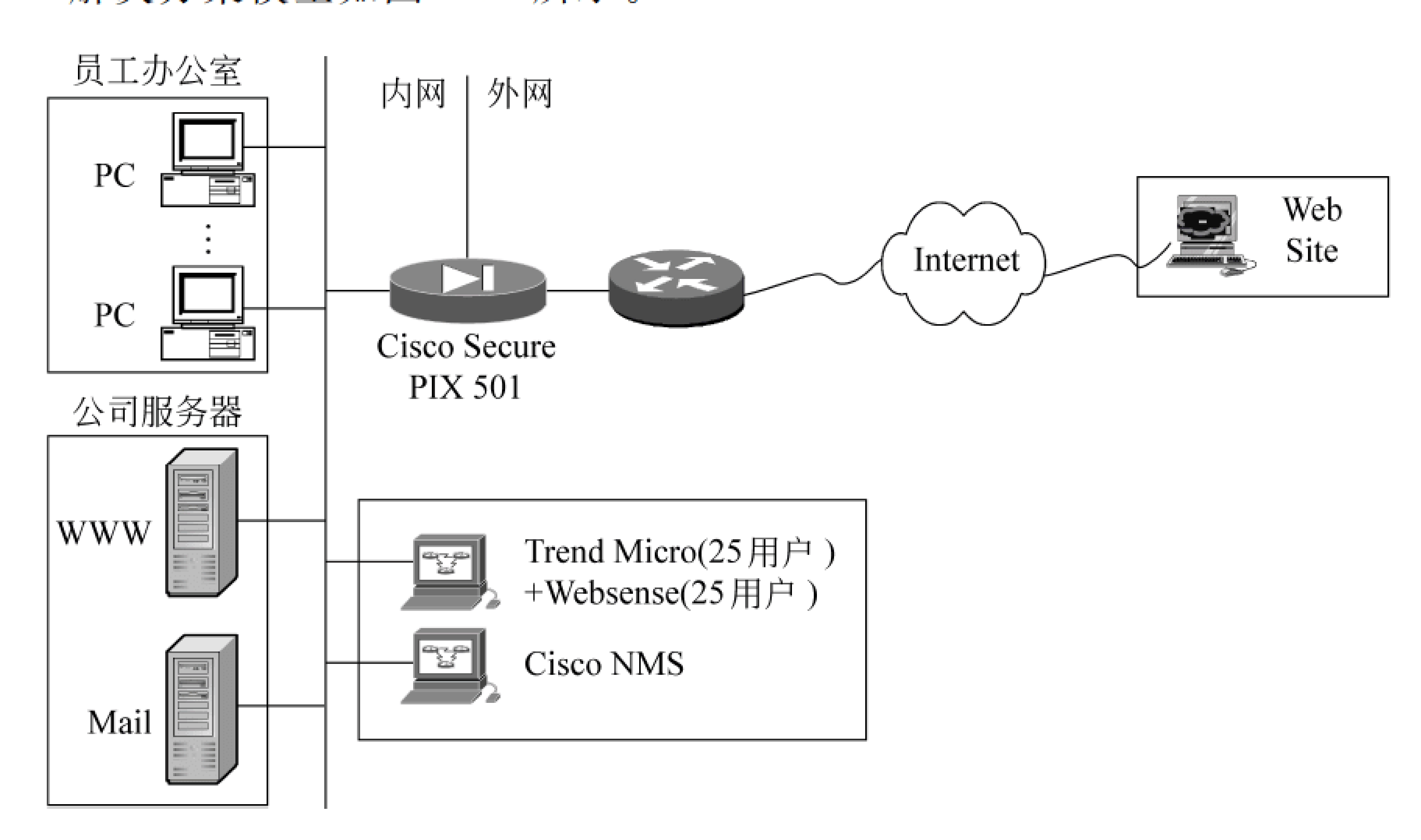



图 7-55　VPN 解决方案

## 7.5 病毒防范系统

病毒自从诞生以来，一直是计算机面临的最大威胁之一，而随着网络特别是互联网的发展，其破坏的威力大大增加。目前，病毒的种类只是一点点地往上增加，并没有往下减少，唯一变化是某一种类的病毒相对来说增长的趋势放缓了，如宏病毒现在变种非常少了，原来的 DoS 病毒现在基本已经没有了。但是过去有引导性的病毒现在也不是完全

消亡了，偶尔也会出现一两个，但是往往是新的种类，如邮件型病毒、蠕虫或者对应系统漏洞进行传播的病毒。现在往往一个病毒具有多种病毒的特点，即通过邮件传播，又攻击系统漏洞。包括去年下半年的熊猫烧香，这些病毒并不是有什么创新，如果说有创新就是把以前的病毒传播方式都学习过来了，采取复合传播、复合攻击方式。在互联网的环境下，病毒对网络安全的危害更加严重，防范也更加困难和复杂。病毒的防范已经成为计算机网络安全体系不可缺少的组成部分。

### 7.5.1 病毒防范的技术措施

在完善的管理措施基础上防治计算机病毒还应有强大的技术支持。对于重要的系统，常用的病毒防治技术措施有系统安全、软件过滤、文件加密、生产过程控制、后备恢复等。

#### 1. 系统安全

许多计算机病毒都是通过系统漏洞进行传播的，如利用 Windows 操作系统漏洞的蠕虫病毒、利用 Outlook 服务软件漏洞的邮件病毒、利用 Office 漏洞的宏病毒。所以，构造一个安全的系统是国内外专家研究的热点。而各种系统的不断升级也正是为了抵御病毒的侵袭，提高系统的防护能力。有效地杀毒软件也可以防御病毒的侵害，现在大多数杀毒软件和工具都具有实施监测系统内存、定期查杀系统磁盘的功能，并可以在文件打开前自动对文件进行检查。除软件防病毒外，采用防病毒卡和防病毒芯片也是十分有效的方法。这是一种软、硬件结合的防病毒方法。防病毒卡和芯片可与系统结合成一体，系统启动后，在加载执行前获得控制权并开始监测病毒，使病毒一进入内存即被查出。同时自身的检测程序固化在芯片中，病毒无法改变其内容，可有效地抵制病毒对自身的攻击。

#### 2. 软件过滤

软件过滤的目的是识别某一类特殊的病毒，以防止它们进入系统和复制传播。这种方法已被用来保护一些大、中型计算机系统。如国外使用的一种 T-cell 程序集，对系统中的数据和程序用一种难以复制的印章加以保护，如果印章被改变，系统就认为发生了非法入侵。又如 Digital 公司的一些操作系统采用 CA-ex-amine 程序作为病毒检测工具，主要用来分析关键的系统程序和内存常驻模块，能检测出多种修改系统的病毒。它采用专家系统对系统参数进行分析，以识别系统的不正常处和未经授权的改变。

#### 3. 文件加密

文件加密是将系统中可执行文件加密，以避免病毒的危害。可执行文件是可被操作系统和其他软件识别和执行的文件。若病毒不能在可执行文件加密前感染该文件，或不能破译加密算法，则混入病毒代码的文件不能执行。即使病毒在可执行文件加密前感染了该文件，该文件解码后，病毒也不能向其他可执行文件传播，从而杜绝了病毒复制。文件加密对防御病毒十分有效，但由于系统开销较大，目前只用于特别重要的系统。为减

小开销，文件加密也可采用另一种简单的方法，将可执行程序作为明文，并对其校验和进行单向加密，形成加密签名块，并附在可执行文件之后。加密的签名块在执行文件执行之前用公密钥解密，并与重新计算的校验和相比较，如有病毒入侵，造成可执行文件改变，则校验和不符，应停止执行并进行校验。

**4. 备份恢复**

数据备份是保证数据安全的重要措施，可以通过与备份文件的比较来判断是否有病毒入侵。当系统文件被病毒侵害，可用备份文件恢复原有系统。数据备份可采用自动方式，也可以采用手动方式；可定期备份，也可以按需备份。数据备份不仅可以用于被病毒侵害的数据恢复，而且可在其他原因破坏了数据完整性以后进行系统恢复。

## 7.5.2 病毒防范的管理措施

除了网络和移动存储设备外，大量的盗版软件和盗版光盘成为病毒在我国广泛流行的主要载体。计算机软件市场的混乱，软件、游戏的非法复制是病毒泛滥的根源之一。同时，加强计算机安全的教育宣传计算机病毒的危害，普及预防计算机病毒的基本知识，提高计算机管理人员的防范意识，制定合理的管理制度，使病毒能够被早发现、早清除是防治计算机病毒的重要手段。下面列出一些简单有效的病毒预防措施。

（1）备好启动盘并设置写保护。在对计算机进行检查修复和手工杀毒时，通常要使用无毒的启动盘，使设备在较为干净的环境下操作。

（2）尽量不用软盘、U 盘、移动硬盘或其他移动存储设备启动计算机而用本地硬盘启动。

（3）定期对重要的资料和系统文件进行备份。可以通过比照文件大小、检查文件个数、核对文件名字来及时发现病毒。

（4）重要的系统文件和磁盘可以通过赋予只读功能避免病毒的寄生和入侵，也可以通过转移文件位置，修改相应的系统配置来保护重要的系统文件。

（5）重要部门的计算机，尽量专机专用与外界隔绝。

（6）尽量避免在无防毒措施的机器上使用软盘、U 盘、移动硬盘、可擦写光盘等可移动的存储设备。

（7）使用新软件时先用杀毒程序检查，减少中毒机会。

（8）安装杀毒软件、防火墙等防病毒工具，并准备一套具有查毒、防毒、解毒及修复系统的工具软件，并定期对软件进行升级、对系统进行查毒。

（9）经常升级安全补丁。80％的网络病毒是通过系统安全漏洞进行传播的，如红色代码、尼姆达等病毒，所以应定期到相关网站去下载最新的安全补丁。

（10）使用复杂的密码。有许多网络病毒是通过猜测简单密码的方式攻击系统的，因此使用复杂的密码可大大提高计算机的安全系数。

（11）不要在 Internet 上随意下载软件。免费软件是病毒传播的重要途径，如果特别需要，必须在下载软件后进行杀毒。

（12）不要轻易打开电子邮件的附件。邮件病毒是当前病毒的主流之一，通过邮件传

播病毒具有传播速度快、范围广、危害大的特点。较妥当的做法是先将附件保存下来,待杀毒软件检查后再打开。

(13) 不要随意借入和借出移动存储设备。在使用借入或返还的这些设备时,一定要通过杀毒软件的检查,避免感染病毒。对返还的设备若有干净备份,应重新格式化后再使用。

了解一些病毒知识,这样就可以及时发现新病毒并采取相应措施,在关键时刻使自己的计算机免受病毒破坏。如定期检查注册表中的下列键值。

(1) HKLM\SOFJWARE\Microsoft\Windows\CurrentVersion\Run

(2) HKLM\SOFTWARE\ Microsoft\Windows\CurrentVersion\Runservices

一旦发现病毒,迅速隔离受感染的计算机,避免病毒继续扩散,并使用可靠的查杀工具进行查杀。必要时需向国家计算机病毒应急中心和当地公共信息网络安全监察部门报告,请专家协助处理。

若硬盘资料已遭破坏,应利用灾后重建的解毒程序和恢复工具加以分析重建受损状态,而不要急于格式化。

对于计算机病毒的防治,不仅是设备维护的问题,而且是一个合理管理的问题。不仅要有完善的规章制度,而且要有健全的管理体制。所以,只有提高认识、加强管理做到措施到位,才能防患未然,减少病毒入侵后所造成的损失。

### 7.5.3 病毒防范体系

防范网络病毒的过程实际上就是技术对抗的过程,反病毒技术也得适应病毒繁衍和传播方式的发展而不断调整。网络防病毒应该利用网络的优势,使网络防病毒逐渐成为网络安全体系的一部分。从防病毒、防黑客和灾难恢复等几个方面综合考虑,形成一整套安全机制,才可以最有效地保障整个网络的安全。今天的网络防病毒解决方案主要从以下几个方面着手进行病毒防治。

#### 1. 以网为本,防重于治

防治病毒应该从网络整体考虑,从方便管理人员的工作着手,透过网络管理 PC。例如,利用网络唤醒功能,在夜间对全网的 PC 进行扫描,检查病毒情况。利用在线报警功能,当网络上哪台机器出现故障、被病毒侵入时,网络管理人员都会知道,从而在管理中心就加以解决。

#### 2. 与网络管理集成

网络防病毒最大的优势在于网络的管理功能,如果没有把网络管理加上,很难完成网络防毒的任务。管理与防范相结合,才能保证系统的良好运行。管理功能就是管理全部的网络设备,从 Hub、交换机、服务器到 PC、软盘的存取和局域网上的信息互通及与 Internet 的接入等。

### 3. 安全体系的一部分

计算机网络的安全威胁主要来自计算机病毒、黑客攻击和拒绝服务攻击等三个方面，因而计算机的安全体系也应从这几个方面综合考虑，形成一整套的安全机制。防病毒软件、防火墙产品、可调整参数能够相互通信形成一整套的解决方案，才是最有效的网络安全手段。

### 4. 多层防御

多层防御体系将病毒检测、多层数据保护和集中式管理功能集成起来，提供了全面的病毒防护功能，从而保证了“治疗”病毒的效果。病毒检测只是病毒防护的支柱，多层次防御软件使用了三层保护功能实时扫描、完整性保护、完整性检验。

后台实时扫描驱动器能对未知的病毒，包括异形病毒和秘密病毒，进行连续的检测。它能对 E-mail 附加部分、下载的 Internet 文件(包括压缩文件)、软盘及正在打开的文件进行实时的扫描检验。扫描驱动器能阻止已被感染过的文件复制到服务器或工作站上。

完整性保护可阻止病毒从一个受感染的工作站扩散到服务器。完整性保护不只是病毒检测，实际上它能制止病毒以可执行文件的方式感染和传播。还可以防止与未知病毒感染有关的文件崩溃和根除。完整性检验使系统无须冗余的扫描并且能提高实时检验的性能。

集中式管理是网络病毒防护最可靠、最经济的方法。多层次防御病毒软件把病毒检测、多层数据保护和集中式管理的功能集成在同一产品内，因而极大地减轻了反病毒管理的负担，而且提供了全面的病毒防护功能。

### 5. 在网关、服务器上防御

大量的病毒针对网上应用程序进行攻击，这样的病毒存在于信息共享的网络介质上，因而要在网关上设防、网络前端实时杀毒。防范手段应集中在网络整体上，在个人计算机的硬件和软件、LAN 服务器、服务器上的网关、Internet 及 Intranet 的 Web site 上层层设防，对每种病毒都实行隔离、过滤。

## 7.5.4 局域网病毒防范

从本质上来看，局域网同样是由一个个网络节点所组成的，节点可以具体为网络服务器和客户机。计算机病毒可以通过各种途径进入网络中的一个节点(包括服务器)，然后再通过局域网进行传播。

### 1. 病毒在局域网的传播形式

病毒在局域网的传播方式归纳为以下几种。

(1) 局域网资源共享。中小型企业组建的局域网多数用于共享资源，而正是由于共享资源的“数据开放性”，造就了病毒感染的有效渠道。

(2) 服务器数据传播病毒。网络中的客户机可以通过服务器和外界联系，而客户机

之间的内部邮件传递也可以通过服务器完成。一旦服务器感染病毒，所有需要经过服务器的数据也会被感染，进而造成整个网络感染病毒的情况。

(3) 客户机之间的数据传递携带病毒。客户机除了和服务器通信之外，相互之间也需要进行数据传递。如果其中一台计算机感染病毒，在与另一台客户机传递数据时，势必会将病毒带给对方。

(4) 客户机带动服务器染毒，进而感染网络中的其他客户机。这种形式可以说是上述三种的综合。网络中的某一台客户机染毒，通过第一种和第三种形式感染服务器，服务器再由第二种形式感染其他客户机。

如果企业使用的是无盘工作站形式，那么病毒的传播将更为简单。因为其“无盘”并非真的“无盘”(它的盘是网络盘)。当运行网络盘上的一个带毒程序时，便将内存中的病毒传染给该程序或通过映像路径传染到服务器的其他的文件上，因此整个“无盘”网络就彻底地被病毒感染了。

### 2. 局域网的病毒防治

局域网的病毒防治应从两个方面入手。

1) 管理上的策略

(1) 加强网络管理员安全管理水平，提高安全意识。由于有的病毒利用系统漏洞进行攻击，所以需要在第一时间内保持系统和应用软件的安全性，保持各种操作系统和应用软件的更新。由于各种漏洞的不断出现，安全不再是一劳永逸的事，所需要的管理水平和安全意识也待提高。

(2) 加强对局域网用户的安全培训，普及防毒知识。杜绝病毒主观能动性起到了很重要的作用。病毒的蔓延经常是由于企业内部员工对病毒的传播方式不够了解。查杀病毒首先要知道病毒到底是什么，它的危害程度如何。知道了病毒危害性，提高了安全意识，杜绝病毒的战役就已经成功了一半。平时，企业要从加强安全意识着手，对日常工作中隐藏的病毒危害提高警觉性，如对来历不明的文件运行前进行查杀、经常升级病毒库、不随意查看陌生的邮件、减少共享文件夹的数量、文件共享时尽量控制权限并设置密码等，都可以很好地防止病毒在网络中的传播。

(3) 建立局域网内部的升级系统，包括各种操作系统的补丁升级，各种常用的应用软件升级，各种杀毒软件病毒库的升级等。

(4) 加强防病毒管理。使用网络扫描软件，经常对整个网络系统做全面的扫描，查找出网络中究竟有哪些服务器和客户机没有安装相应的防病毒软件。采取强制性的措施为该客户机安装相应的防病毒软件，以确保网络内部没有防病毒漏洞。对已经被病毒感染的计算机在清除之前与整个网络隔离，杜绝网络内计算机带病毒运行。

(5) 建立灾难备份系统。对于数据库和数据系统，必须采用定期备份、多机备份措施，防止意外灾难下的数据丢失。

2) 技术上的策略

应利用全方位的企业防毒产品，实施“层层设防、集中控制、以防为主、防杀结合”的策略。具体而言，就是针对网络中所有可能的病毒攻击，设置对应的防毒软件。通过全

方位、多层次的防毒系统配置，使网络没有薄弱环节成为病毒入侵的缺口。具体配置如图 7-56 所示。

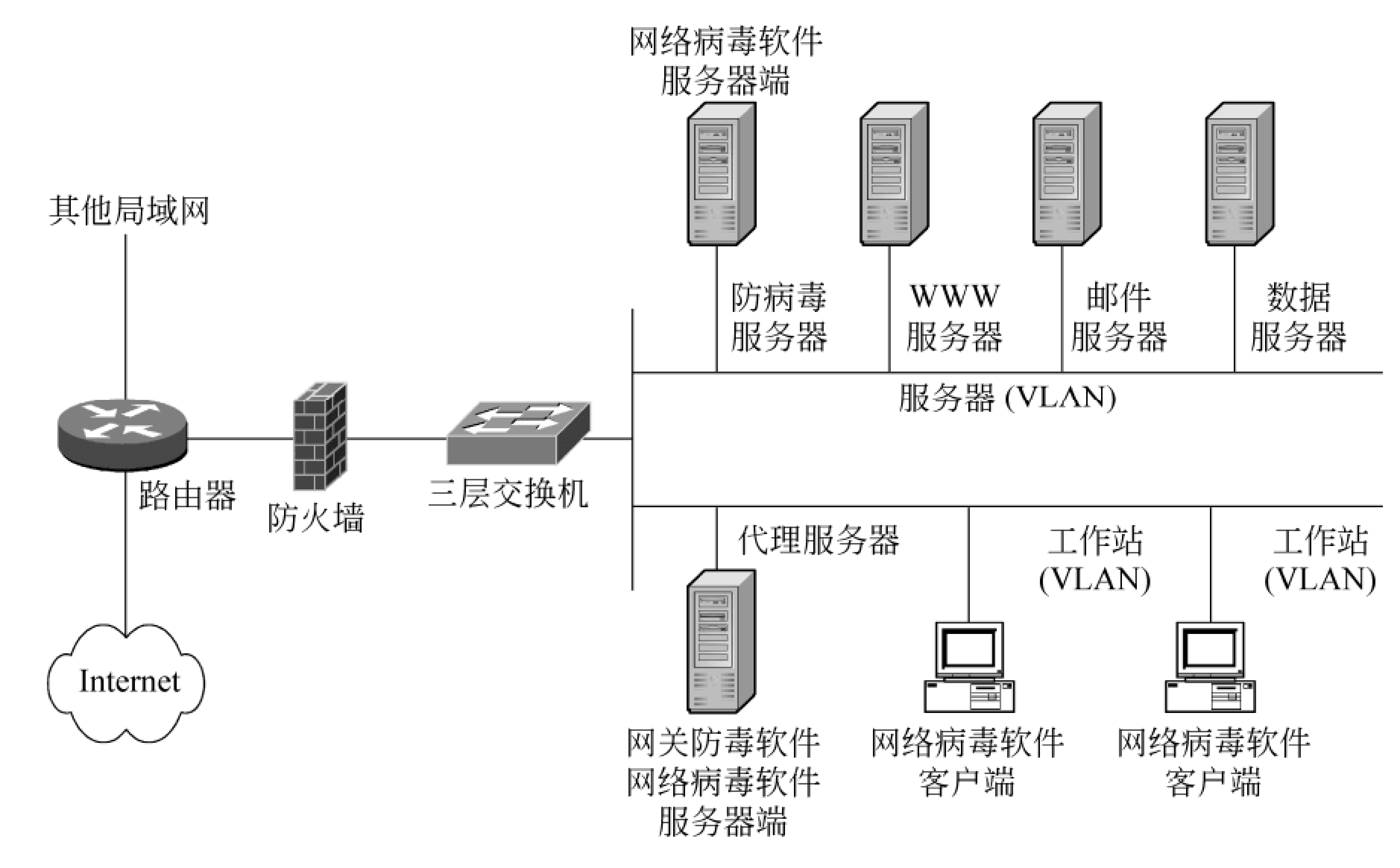



**图 7-56　局域网防范病毒配置**

(1) 防护桌面系统

客户端的防护位于局域网防毒体系的最底层，对用户而言，也是最显而易见的一道防杀病毒的防线。

① 启用 BIOS 引导扇区保护。通过系统的 BIOS 设置打开引导扇区保护功能，可以保证所有系统的引导扇区处于安全状态。系统管理员应对局域网用户进行教育，使他们明白引导扇区警告的含义，以及如何进行相应的处理。

② 安装网络版杀毒软件客户端。通过服务器设置统一的防毒策略，定期对本地驱动器进行彻底的病毒扫描，定期自动更新病毒库，获取完整的病毒活动日志，防止病毒从客户机进入系统，实现客户端的实时病毒防护，保护客户机自身不会被病毒感染，并且不会成为病毒源。

(2) 防护服务器

服务器会遭受大量引导型病毒、文件型病毒、混合型病毒、蠕虫以及宏病毒等的攻击。更为常见的是，由于服务器为网络中所有工作站提供共享的资源，因而也成为病毒理想的集散地，可以轻易将病毒扩散到网络中的所有工作站或服务器上。

① 设置防病毒服务器，安装网络版杀毒软件。在网络内部设置一台防病毒主控服务器，负责病毒特征码的分发和整个网络防病毒软件的管理。每天晚上应对每台服务器的所有文件都使用病毒扫描程序进行彻底的扫描。多数网络版杀毒软件都带有日程安排功能，可以自动进行扫描。开启实时病毒监控功能、病毒码自动更新功能以及病毒活动日志、多种报警通知方式等。

② 设置文件权限。设置用户级的文件权限可以保证服务器的可执行文件不被感染。

(3) Internet 网关的防护

Internet 网关的病毒防护是局域网防病毒体系结构中的重要组成部分，它可以为局域网提供更完整的保护。其基本设计理念是在计算机病毒通过 Internet 来入侵企业内部网络的第一点处设置一道防毒墙，使得计算机病毒在进入企业网络之前即被阻截。保证网络用户在使用浏览器、FTP 下载和收发邮件时免遭各种病毒，特别是 Java Applet、ActiveX 和未标记的 Web 对象等新一代病毒的侵害。推荐使用代理服务器，并在该服务器中安装网关防病毒软件，既可以对外部入侵病毒进行监测和拦截，又可以为服务器多加一层保护。

(4) 防毒中央控管系统

较好的网络版杀毒软件都支持网络集中管理，这样在域中的某台机器上就可以管理整个网络，进行全域的监控、查毒、防毒、杀毒等各种工作。另外，还可以通过点到点的方法来管理远程的不同网段上的计算机，这避免了系统管理人员分别去处理每一台机器，极大地减轻管理员的工作量，减少了大量的重复操作，方便了管理。

用一台服务器(可以不是主域服务器)作为防病毒服务器对整个域进行防病毒管理，制定统一的防毒策略，设定域扫描作业，安排系统自动查、杀病毒。定时自动下载最新病毒特征文件和搜索引擎，然后自动分发到域中其他服务器和联网客户机上，保证防毒软件定期得到最新的反病毒文件。

(5) 划分虚拟局域网(VLAN)

经济条件许可时，局域网内应尽量使用支持虚拟局域网(VLAN)的交换设备，最好是三层的(支持路由功能)，将各小部门划分成子网。设置独立的服务器，杜绝网络内部大范围的共享文件夹和硬件资源，这在保护数据安全和防毒上均可起到相当的作用。

## 7.5.5 手工清除病毒措施

现在上网的用户越来越多了，其中有一点不可避免的就是如何防范和查杀病毒和恶意攻击程序。但是，如果不小心中了病毒而身边又没有杀毒软件怎么办？没有关系，下面所述的方法可以轻松地手工清除藏在计算机里的病毒和木马。

### 1. 检查注册表

注册表一直都是很多木马和病毒“青睐”的寄生场所，注意在检查注册表之前要先给注册表备份。

(1) 检查注册表中 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 和 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runserveice，查看键值中有没有不熟悉的自动启动文件，扩展名一般为 EXE，然后记住程序的文件名，在整个注册表中搜索，凡是看到了一样的文件名的键值就要删除，接着到计算机中找到木马文件的藏身地将其彻底删除。例如“爱虫”病毒会修改上面所提的第一项，BO2000 木马会修改上面所提的第二项。

(2) 检查注册表 HKEY_LOCAL_MACHINE 和 HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main 中的几项(如 Local Page)，如果发现键

值被修改了，只要根据判断改回去就行了。恶意代码（如“万花谷”）就经常修改这几项。

（3）检查 HKEY_CLASSES_ROOT\inifile\shell\open\command 和 HKEY_CLASSES_ROOT\txtfile\shell\open\command 等几个常用文件类型的默认打开程序是否被更改。这个一定要改回来，很多病毒就是通过修改.txt、.ini 等的默认打开程序而清除不了的。例如“罗密欧与朱丽叶”病毒就修改了很多文件（包括.jpg、.rar、.mp3 等）的默认打开程序。

### 2. 检查系统配置文件

其实检查系统配置文件最好的方法是打开 Windows 系统配置实用程序（从“开始”菜单运行 msconfig.exe），在里面可以配置 Config.sys、Autoexec.bat、system.ini 和 win.ini，并且可以选择启动系统的时间。

（1）检查 win.ini 文件（在 C:\Windows\下），打开后在[WINDOWS]的下面，“run=”和“load=”是可能加载“木马”程序的途径，必须仔细留心它们。在一般情况下，在它们的等号后面什么都没有，如果发现后面跟有路径与文件名不是熟悉的启动文件，计算机就可能中上“木马”了。例如攻击 QQ 的“GOP 木马”就会在这里留下痕迹。

（2）检查 system.ini 文件（在 C:\Windows\下），在 BOOT 下面有个“shell=文件名”。正确的文件名应该是 explorer.exe，如果不是 explorer.exe，而是“shell= explorer.exe 程序名”，那么后面跟着的那个程序就是“木马”程序，然后就要在硬盘找到这个程序并将其删除了。这类的病毒很多，例如“尼姆达”病毒就会把该项修改为 shell=explorer.exe load.exe-dontrunold。

网络由于自身在很多方面存在天生的缺陷，造成网络安全是非常脆弱的，而且这种脆弱是全方位的。针对网络安全所受到的主要威胁，目前构建网络安全体系涉及防火墙、入侵检测与防御系统、身份认证系统、虚拟专网以及病毒防范系统等很多方面。在采用相关系统时，应注意在工作原理、技术分类、如何部署以及采购相关产品时给予更多关注。

## 习　题　7

（1）常见的认证技术有哪些？各有什么特点？

（2）简述 802.1x 认证技术的实现。

（3）目前计算机病毒有哪些特点？如何建立比较完善的防病毒体系？

（4）防火墙在网络中具有哪些作用和缺陷？

（5）如何部署防火墙？

（6）简述虚拟专网的分类和用途。

（7）什么是入侵检测系统？有哪几类技术？

（8）典型的入侵检测方法有哪几类？

# 第8章 chapter 8

# 网络安全系统解决方案

网络安全是一项系统工程，它既涉及对外部攻击的有效防范，又包括制定完善的内部安全保障制度来防范内部的网络攻击；既涉及防病毒攻击，又涵盖网络攻击检测、防黑客攻击等内容。因此，网络安全解决方案不应仅仅提供对某种安全隐患的防范能力，而是应涵盖对于各种可能造成网络安全的各个方面的隐患提供整体的防范能力。网络安全不仅涉及网络系统的多个层次和多个方面，而且还是一个动态变化的过程，因此它还应该是一种动态解决和动态适应的方案，能够随着网络安全需求的变化而不断改进完善。

网络安全涉及到许多方面，最明显、最重要的就是对外界入侵、攻击的检测与防护。现在的网络几乎时刻受到外界的安全威胁，稍有不慎就会被那些病毒、黑客入侵，致使整个网络陷入瘫痪。在一个安全措施完善的计算机网络中，不仅要部署病毒防护系统、防火墙隔离系统，还可能要部署入侵检测、木马查杀系统和物理隔离系统等。当然所选用系统的具体等级要根据相应网络规模大小和安全需求而定，并不一定要求每个网络系统都全面部署这些防护系统。

除了病毒、黑客入侵外，网络系统的安全性需求还体现在用户对数据的访问权限上，一定要根据对应的工作需求为不同用户、不同数据配置相应的访问权限，对安全级别需求较高的数据则要采取相应的加密措施。同时，用户账户，特别是高权限账户的安全也应受到高度重视，要采取相应的账户防护策略（如密码复杂性策略和账户锁定策略等），保护好用户账户，以防被非法用户盗取。

## 8.1 网络安全系统整体实施概述

计算机网络安全的实质是安全立法、安全管理和安全技术的综合实施。这三个层次体现了安全策略的限制、监视和保障职能。所以，网络安全是一项涉及众多方面的系统工程，既需要被动防御，又需要主动防御；既需要采取必要的安全技术来抵御各种攻击，又需要规范和建立必要的安全管理模式、规章制度等来规范人们的行为。在这里主要从技术角度讨论如何具体应用前面已经论述的网络安全策略。

### 8.1.1 网络安全系统的构架

ITU-T X.800 标准将常说的网络安全(networksecurity)进行逻辑上的分别定义,即安全攻击(security attack)是指损害机构所拥有信息的安全的任何行为;安全机制(security mechanism)是指设计用于检测、预防安全攻击或者恢复系统的机制;安全服务(security service)是指采用一种或多种安全机制以抵御安全攻击、提高机构的数据处理系统安全和信息传输安全的服务。三者之间的关系如表 8-1 所示。

**表 8-1 安全攻击、安全机制、安全服务之间的关系**

| 释放消息内容 | 流量分析 | 伪装 | 重放 | 更改消息 | 拒绝服务 | 安全攻击 / 安全机制 / 安全服务 | 加密 | 数字签名 | 访问控制 | 数据完整性 | 认证交换 | 流量填充 | 路由控制 | 公证 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | √ | | | | 对等实体认证 | √ | √ | | | √ | | | |
| | | √ | | | | 数据源认证 | √ | √ | | | | | | |
| | | √ | | | | 访问控制 | | | √ | | | | | |
| √ | | | | | | 机密性 | √ | | | | | | √ | |
| | √ | | | | | 流量机密性 | √ | | | | | √ | √ | |
| | | | √ | √ | | 数据完整性 | √ | √ | | √ | | | | |
| | | | | | | 非否认性 | | √ | | √ | | | | √ |
| | | | | | √ | 可用性 | | | | √ | √ | | | |

#### 1. 网络安全防范体系框架结构

为了能够有效了解用户的安全需求,选择各种安全产品和策略,有必要建立一些系统的方法来进行网络安全防范。网络安全防范体系的科学性、可行性是其可顺利实施的保障。图 8-1 给出了基于 DISSP(美国国防信息系统安全计划)扩展的一个三维安全防范技术体系框架结构。第一维是安全服务,给出了八种安全属性(ITU-T REC-X. 800-199103-I)。第二维是系统单元,给出了信息网络系统的组成。第三维是结构层次,给出并扩展了国际标准化组织 ISO 的开放系统互联(OSI 模型)。

框架结构中的每一个系统单元都对应于某一个协议层次,需要采取若干种安全服务才能保证该系统单元的安全。网络平台需要有网络节点之间的认证、访问控制,应用平台需要有针对用户的认证、访问控制,需要保证数据传输的完整性和保密性,需要有抗抵赖和审计的功能,需要保证应用系统的可用性和可靠性。针对一个信息网络系统,如果在各个系统单元都有相应的安全措施来满足其安全需求,则认为该信息网络是安全的。

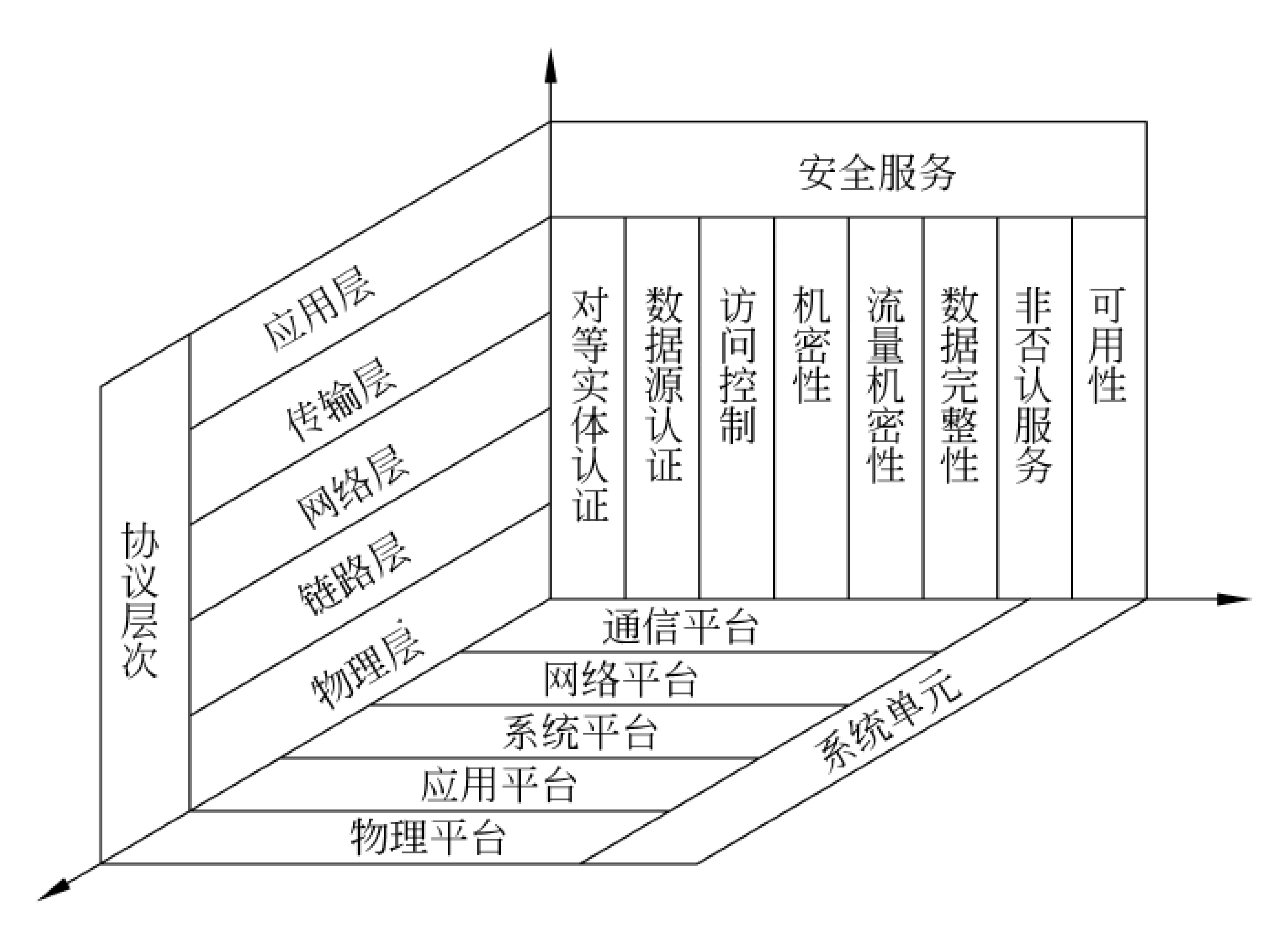



**图 8-1　三维安全防范技术体系框架结构**

### 2. 网络安全防范体系层次

作为全方位的、整体的网络安全防范体系也是分层次的，不同层次反映了不同的安全问题。根据网络的应用现状和网络的结构，将安全防范体系的层次（见图 8-2）划分为物理层安全、系统层安全、网络层安全、应用层安全和安全管理。

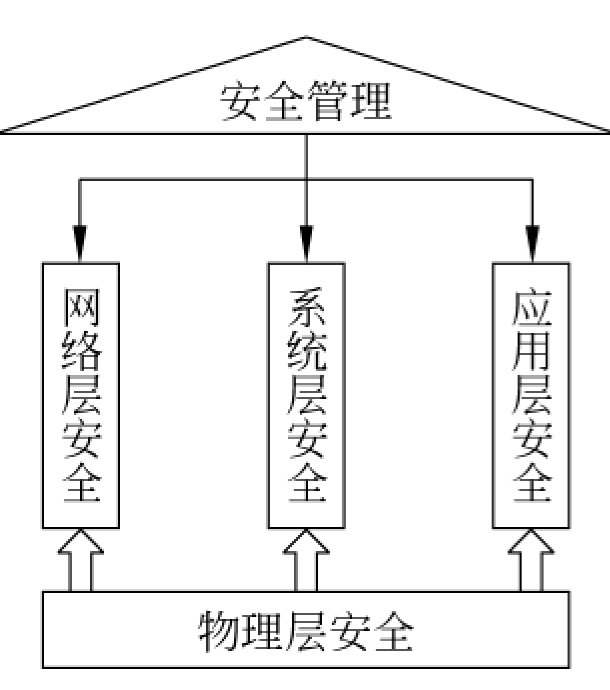



**图 8-2　网络安全防范体系层次**

1）物理环境的安全性——物理层安全

该层次的安全包括通信线路的安全、物理设备的安全、机房的安全等。物理层的安全主要体现在通信线路的可靠性、线路备份、网管软件、传输介质；软硬件设备安全性、交换设备、拆卸设备、增加设备；设备的备份；防灾害能力、防干扰能力；设备的运行环境（温度、湿度、烟尘、不间断电源保障）等。

2）操作系统的安全性——系统层安全

该层次的安全问题来自网络内使用的操作系统的安全，如 Windows Server 2000、Windows Server 2003 等。主要表现在三方面：一是操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制、系统漏洞等；二是对操作系统的安全配置问题；三是病毒对操作系统的威胁。

3）网络的安全性——网络层安全

该层次的安全问题主要体现在网络方面的安全性，包括网络层身份认证、网络资源的访问控制、数据传输的保密与完整性、远程接入的安全、域名系统的安全、路由系统的安全、入侵检测的手段、网络设施防病毒等。

4）应用的安全性——应用层安全

该层次的安全问题主要由提供服务所采用的应用软件和数据的安全性产生，包括 Web 服务、电子邮件系统、DNS 等。此外，还包括病毒对系统的威胁。

5）管理的安全性——安全管理

安全管理包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制度化极大程度地影响着整个网络的安全，严格的安全管理制度、明确的部门安全职责划分、合理的人员角色配置都可以在很大程度上降低其他层次的安全漏洞。

### 3. 现代网络安全体系模型

根据网络安全目前的局势和网络安全技术的发展，网络安全体系正从传统的静态被动防范向动态主动防范方向发展。图 8-3 是动态主动防范安全系统的管理模型。其基本思路是根据制定安全防范策略，检测网络中的各种活动，调查和鉴别发现的问题，并将分析结果通知网络安全设备作为响应条件，网络安全设备根据接收到的分析结果采取相应措施，加入保护、跟踪、恢复等动作。

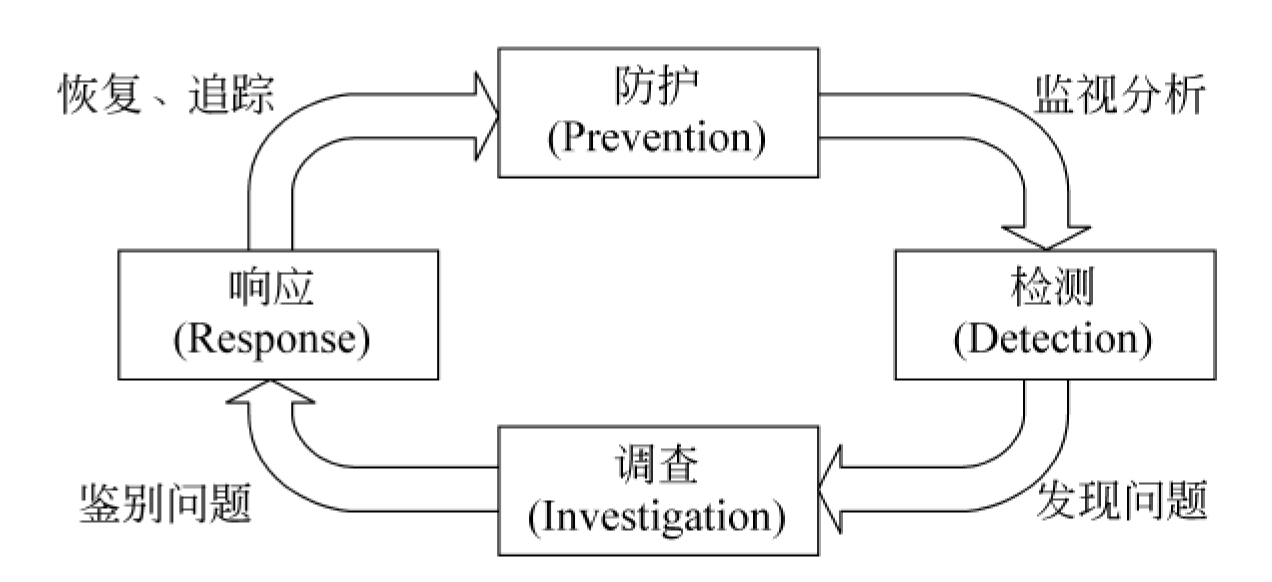



**图 8-3 现代网络安全体系模型**

基于以上网络安全体系模型，构建网络安全体系结构，如图 8-4 所示。在进行网络风险分析的基础上，制定全网的安全策略，利用统一的网络安全管理平台分发安全策略，实现全网安全策略的部署，采用在线检测技术，监控全网的网络动态，并依据检测分析结果采取快速隔断、分级保护、封闭和恢复等措施，形成网络设备和专业网络安全分工协作共同保证网络安全的局面。

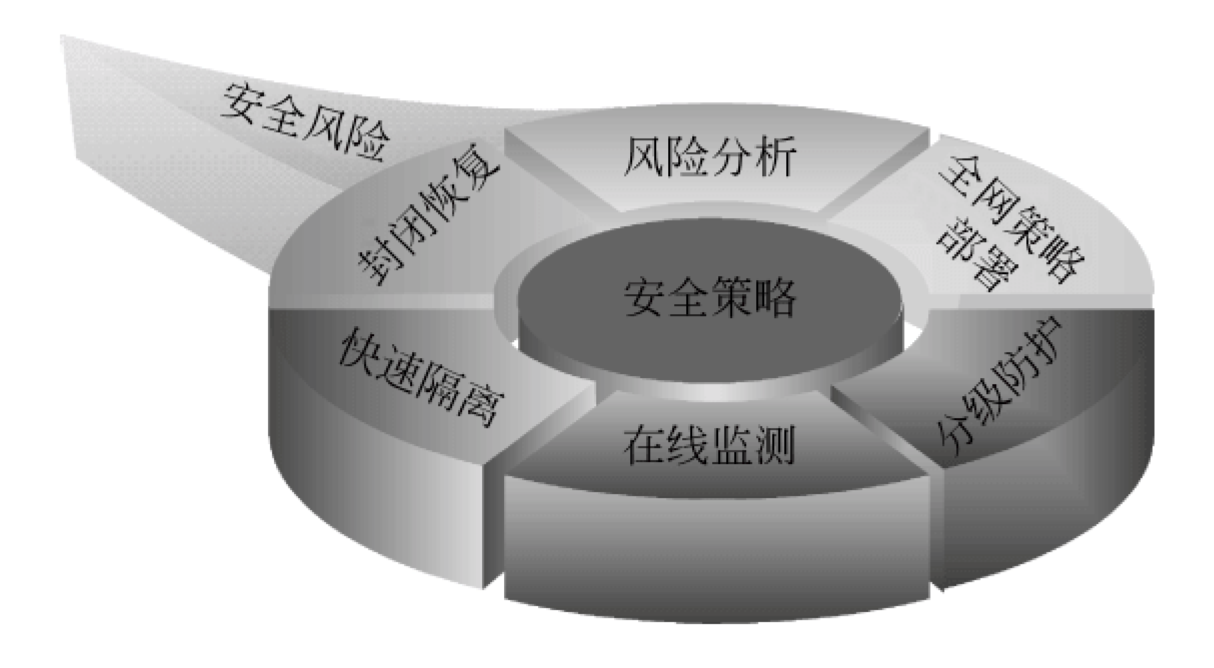



**图 8-4 网络安全系统结构**

## 8.1.2 网络安全系统设计的基本原则

目前，对于新建网络及已投入运行的网络，在进行网络安全系统设计时应遵循如下思想：大幅度地提高系统的安全性和保密性；保持网络原有的性能特点，即对网络的协议

和传输具有很好的透明性；易于操作、维护，并便于自动化管理，不增加或少增加附加操作；尽量不影响原网络拓扑结构，便于系统及系统功能的扩展；安全保密系统具有较好的性能价格比，一次性投资，可以长期使用；安全与密码产品具有合法性，并便于安全管理单位与密码管理单位的检查与监督。

基于上述思想，网络安全系统应遵循如下设计原则。

**1. 满足 Internet 的分级管理需求**

根据 Internet 网络规模大、用户众多的特点，对 Internet/Intranet 信息安全实施分级管理的解决方案，将对它的控制点分为三级实施安全管理。

（1）中心级，主要实现内外网隔离，内外网用户的访问控制，内部网的监控，内部网传输数据的备份与稽查。

（2）部门级，主要实现同级部门间的访问控制，部门网内部的安全审计。

（3）终端/个人用户级，实现部门内部主机的访问控制，数据库及终端信息资源的安全保护。

**2. 需求、风险、代价平衡的原则**

对任一网络，绝对安全是难以达到的，也不一定是必要的。对一个网络进行实际的研究（包括任务、性能、结构、可靠性、可维护性等），并对网络面临的威胁及可能承担的风险进行定性与定量相结合的分析，然后制定规范和措施，确定本系统的安全策略。

**3. 综合性、整体性原则**

应用系统工程的观点和方法，分析网络的安全及具体措施。安全措施主要包括：行政法律手段、各种管理制度（人员审查、工作流程、维护保障制度等）以及专业措施（识别技术、存取控制、密码、低辐射、容错、防病毒、采用高安全产品等）。一个较好的安全措施往往是多种方法适当综合的应用结果。一个计算机网络，包括个人、设备、软件、数据等，这些环节在网络中的地位和影响作用，也只有从系统综合整体的角度去看待、分析，才能取得有效可行的措施。计算机网络安全应遵循整体安全性原则，根据规定的安全策略制定出合理的网络安全体系结构。

网络安全系统的整体性是要求在网络发生被攻击、破坏事件的情况下，必须尽可能地快速恢复网络信息中心的服务，减少损失。因此，信息安全系统应该包括安全防护机制、安全检测机制和安全恢复机制。安全防护机制是根据具体系统存在的各种安全威胁采取相应的防护措施，避免非法攻击的进行。安全检测机制是检测系统的运行情况，及时发现和制止对系统进行的各种攻击。安全恢复机制是在安全防护机制失效的情况下，进行应急处理和尽量及时地恢复信息，减少供给的破坏程度。

**4. 可用性原则**

安全措施需要人为去完成，如果措施过于复杂，要求过高，本身就降低了安全性，如密钥管理就有类似的问题。其次，措施的采用不能影响系统的正常运行，如不采用或少

采用极大地降低运行速度的密码算法。

**5. 分步实施原则**

由于网络系统及其应用扩展范围广阔，随着网络规模的扩大及应用的增加，网络脆弱性也会不断增加，一劳永逸地解决网络安全问题是不现实的。同时由于实施信息安全措施需相当的费用支出，因此分步实施，既可满足网络系统及信息安全的基本需求，亦可节省费用开支。

**6. 木桶原则**

网络安全的木桶原则是指对信息均衡、全面的进行保护。“木桶的最大容积取决于最短的一块木板”。网络系统是一个复杂的计算机系统，它本身在物理上、操作上和管理上的种种漏洞构成了系统的安全脆弱性，尤其是多用户网络系统自身的复杂性、资源共享性使单纯的技术保护防不胜防。攻击者使用的“最易渗透原则”，必然在系统中最薄弱的地方进行攻击。因此，充分、全面、完整地对系统的安全漏洞和安全威胁进行分析，评估和检测包括模拟攻击是设计信息安全系统的必要前提条件。安全机制和安全服务设计的首要目的是防止最常用的攻击手段，根本目的是提高整个系统的“安全最低点”的安全性能。

**7. 标准化与一致性原则**

网络系统是一个庞大的系统工程，其安全体系的设计必须遵循一系列的标准，这样才能确保各个分系统的一致性，使整个系统安全地互联互通、信息共享。

**8. 技术与管理相结合原则**

安全体系是一个复杂的系统工程，涉及人、技术、操作等要素，单靠技术或单靠管理都不可能实现。因此，必须将各种安全技术与运行管理机制、人员思想教育与技术培训、安全规章制度建设相结合。

**9. 动态发展原则**

要根据网络安全的变化不断调整安全措施，适应新的网络环境，满足新的网络安全需求。

**10. 易操作性原则**

首先，安全措施需要人为去完成，如果措施过于复杂，对人的要求过高，本身就降低了安全性。其次，措施的采用不能影响系统的正常运行。

### 8.1.3 网络安全系统设计的基本方法

设计一个网络安全系统并非那么简单。对设计标准的评价会让人理解网络及其作用，网络安全设计必须适应下一代技术的实施。网络安全系统设计规划并不是仅为新的

网络而做，而是在现有基础上的改进。网络安全设计如果是基于稳定的结构而很好地规划，以后重新设计时就会很容易。

设计只是网络生命周期的一个部分。规划、设计、实施、操作和优化（planning、design、implementation、operation、optimization，PDIOO）构成了完整的网络生命周期，每个阶段都是在前阶段基础上建立起一个强健的网络，即便业务需求发生变化，也能保持网络的有效性。PDIOO 方法可以运用到所有技术上。在 PDIOO 期间，可以定义出关键的系统模块以及相关的技术，这些技术与增加客户网络价值有着直接的联系。例如，理解业务目标、使用特性和网络需求，将有助于避免不必要的升级和网络再设计，因而能够减少将一个新服务引入网络而需要的时间。

**1. 规划阶段**

在规划阶段，可以对将来的设计逻辑进行测试以发现问题。规划有助于避免重复网络设计当中的逻辑性错误，因为这些网络设计模板可能会在很多地方使用。规划阶段的焦点是技术和投资标准，并且要考虑到本章前面提到的需求和制约。在规划阶段，识别出所有的用户需求是很重要的。

**2. 设计阶段**

完成规划之后就有足够的信息来开发网络设计了。如果是一个现成的网络，设计阶段的工作应该是去复查和验证。在设计阶段，可以选择产品、协议，并且基于规划阶段确定的标准来选择特性。可以开发网络图来演示为取得既定效果对网络要做哪些更改。设计和规划越详细，也就越能提前预见实施过程中可能会碰到的挑战。

**3. 实施阶段**

实施阶段提供详细的、定制的计划，有助于避免风险并满足期望。一个强健的实施计划能够确保即使问题出现也平稳部署。与所有用户进行沟通，以便评估计划的有效性。在草案阶段及早发现问题要比实施时才发现要好得多。

像变更控制这样好的流程可以有效解决部署阶段碰到的问题，变更控制提供了一定的灵活性，因为要对每个偶然现象都做出计划显然是不可能的，特别是长期的实施过程。

**注意**：变更控制是一个组织业务流程实施授权变更的过程，这其中牵涉到对问题的分析和在正式建议中增加一些成果。这种建议应该在授权之前得到管理层的复查。

**4. 操作阶段**

操作阶段，也被称做操作支持阶段，主要目的是保护网络投资，防止问题，最大化系统的功用，提升问题解决的能力。

**5. 优化阶段**

PDIOO 的最后一个阶段是优化网络。一个强健的设计是需要优化和调整的，以便

充分发挥其潜能。优化可以是对服务器做简单的安全加固，也可以是针对延迟敏感的流量增加网络的 QoS。图 8-5 显示了 PDIOO 过程，每个阶段都是前后关联的。

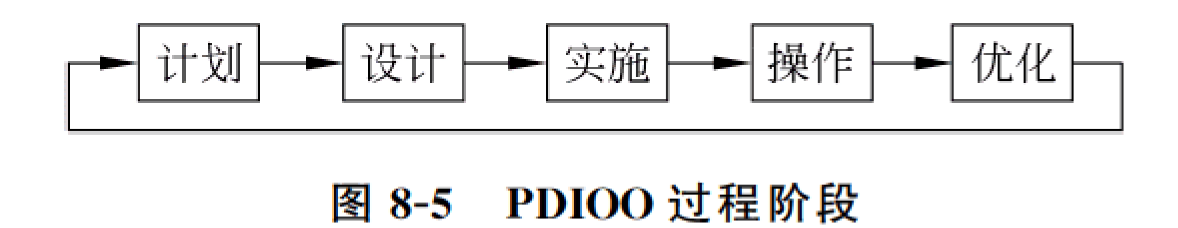



**图 8-5 PDIOO 过程阶段**

优化甚至能够引发网络的重新设计，致使开始一次新的循环。

## 8.2 无线局域网的安全策略

随着互联网不断发展和移动办公需求越来越大，人们希望能够摆脱有线网络的束缚，能够在任何地点、任何时间方便快捷地接入网络，而无线网络技术的实现满足了人们的这种愿望，而且随着无线网络技术的快速进步，无线网络已经从计算机网络的补充角色在向计算机网络的主要形势转换。但无线网络固有的工作原理，使得网络安全变得比有线网络更为严峻。在无线网络给人们带来种种便利的同时，也为黑客对基于无线链路和智能移动终端的蓄意破坏、篡改、窃听、假冒、泄露和非法访问信息资源的各种攻击行为提供了方便。另外，由于网络本身体系结构复杂、传输速度慢、信号容易受感染、安全隐患多，也使得无线网络的安全措施更为迫切和困难。

### 8.2.1 无线局域网的工作原理

**1. 什么是无线局域网（WLAN）**

无线局域网（wireless LAN，WLAN）通常部署在校园、小区、企业办公室、会议室、工业仓库、网络教室和咖啡厅。按照 IEEE 802.11 标准中的定义，WLAN 使用空气中的无线电频率（RF）作为介质发送和接收数据。

基于 IEEE 802.11 的 WLAN 给网络管理员和信息安全管理员带来了新的挑战。传统的有线以太网部署相对简单，与之不同的是，802.11 WLAN 向客户工作站广播 RF 信号，以便它们监听。

为更好地理解 WLAN 的弱点和带来的挑战，图 8-6 针对一个无线网络环境下的客户机/服务器应用描述了 802.11 标准的协议栈。

IEEE 802.11 标准说明了无线客户端和基站（AP）之间的接口以及无线客户端之间连接的接口。与其他 802.x 系列标准（802.3 是以太网，802.5 是令牌环网）类似，802.11 提供了物理层（PHY）和介质访问控制（MAC）层的标准。

802.11 标准最早在 1997 年发布，定义了 MAC 层、MAC 层管理协议和服务以及 3 种不同数据速率的物理层。后续的版本在数据速率、安全功能和服务质量（QoS）等方面有了提高。表 8-2 比较了不同标准间的主要区别。

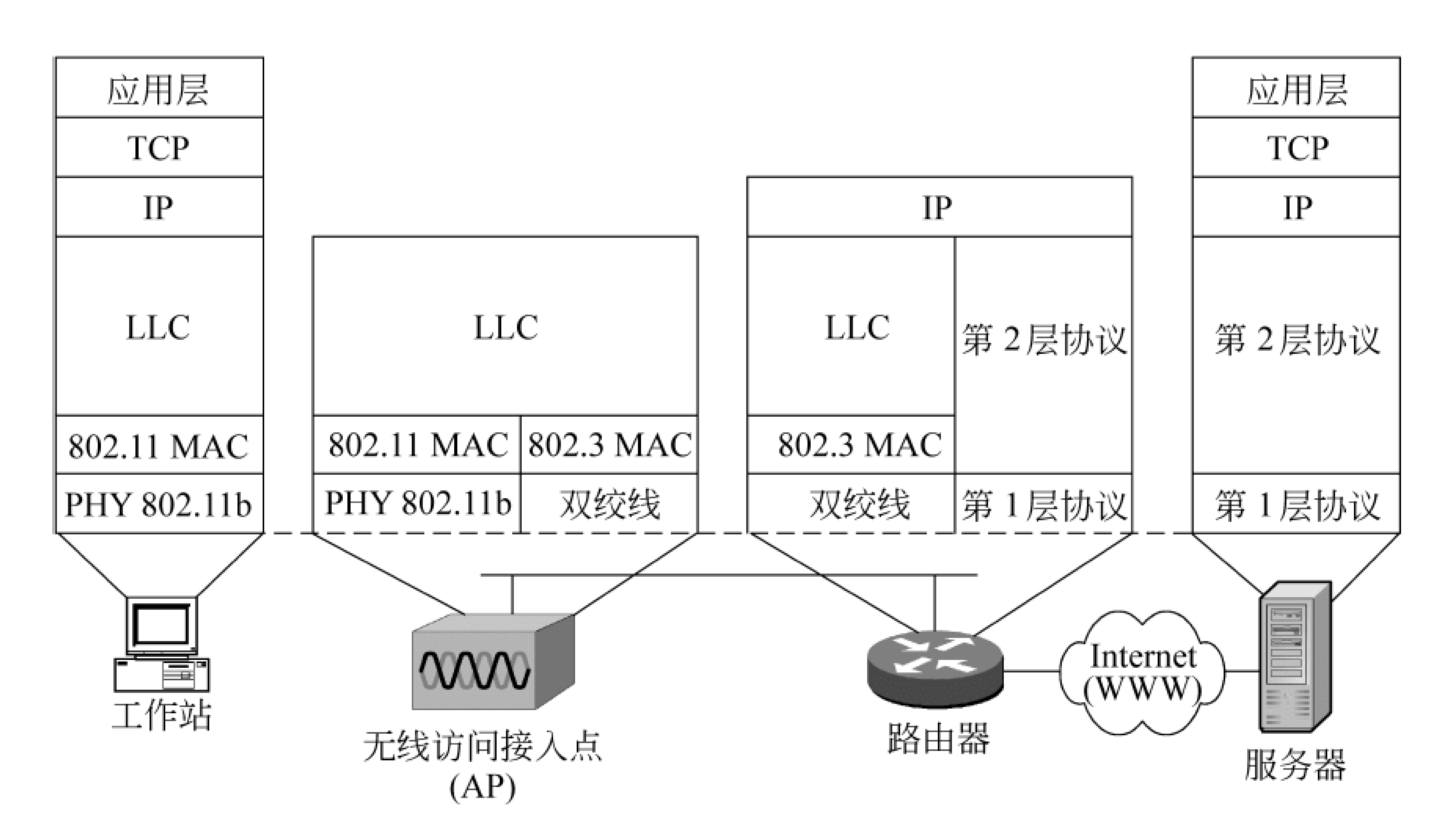



**图 8-6　802.11 协议栈**

**表 8-2　802.11 标准概述**

| | **802.11a** | **802.11b** | **802.11g** | **802.11n** |
|---|---|---|---|---|
| 频率 | 5GHz | 2.4GHz | 2.4GHz | 2.4GHz/5GHz |
| 速度 | 54Mbit/s | 11Mbit/s | 54Mbit/s | 108Mbit/s 以上 |
| 市场应用 | 家庭娱乐 | 无线办公室 | 家庭或办公应用 | 园区网 |

802.11a 和 802.11g 的数据传输速度是相同的，但 5GHz 的频带有一些局限，在有些国家不如 2.4GHz 频带清晰。目前还存在些其他 802.11 标准或正在定义新的标准。本章节将重点讨论 802.11i，它增强了 802.11 的 MAC 层，提高了安全性和认证机制。

**2. 无线网络的工作原理**

应用于 802.11a/b/g WLAN 标准的安全，研发人员和黑客都发现了一些标准中所定义的认证、数据保密性和消息完整性机制的漏洞。为更好地理解这些漏洞，本节详细介绍无线网络的工作原理。

1）WLAN 的体系结构

WLAN 的体系结构由 3 个部分构成：无线客户端工作站；无线访问接入点 AP；基本服务集（basic service set，BSS）。无线客户端工作站可以是任何采用 802.11 标准通信的设备（如笔记本电脑、工作站、PDA 甚至打印机和扫描仪）。访问接入点（AP）提供两个功能：一方面作为 WLAN 和有线 LAN 之间的连接平台，另一方面作为所有连接该 AP 的无线客户端工作站的中继。

无线工作站和 AP 都是物理设备部件，基本服务集 BSS 是无线体系结构中的逻辑部件。BSS 通常是一些无线工作站的集合，它们由一个简单管理功能所控制，BSS 具有两种配置选项。在自主基本服务集（IBSS）中，工作站之间不需要 AP 直接进行通信。扩展服务集（extended service set，ESS）是一系列基础结构基本服务集的集合，形成一个单个

的基本服务集，这对提供冗余连接是非常重要的，但也存在一些安全问题需要解决。

2）建立 WLAN 连接

由于 WLAN 使用无线电频率发送和接收数据，因此建立无线连接的第一个步骤是进行信号扫描。类似于调谐一个无线电台，扫描功能是指一个无线工作站查找另一个工作站或 AP。802.11 标准定义了两类扫描功能：主动扫描和被动扫描。在扫描过程中，工作站监听信号帧(beacon frames，类似于保持活动 keepalive 消息)，以定位和识别在区域内的 BSS。信号帧中包含的信息有服务集标识符(service set identifiers，SSID)、支持的速率以及时间戳。

图 8-7 说明了建立连接的步骤，下面讨论认证过程的每个步骤。802.11 标准规定了开放认证和共享密钥认证两类认证客户端的机制，通常也采用 SSID 认证和客户端 MAC 认证两种认证方式。这些机制的缺陷在后面的无线风险节中介绍。有线等效加密(wired equivalent privacy，WEP)密钥可作为一种访问控制方法，如果一个客户端没有正确的 WEP 密钥，就无法和 AP 间发送和接收数据。IEEE 802.11 委员会采用了 WEP 加密算法，支持 40 位和 128 位两种长度的密钥。

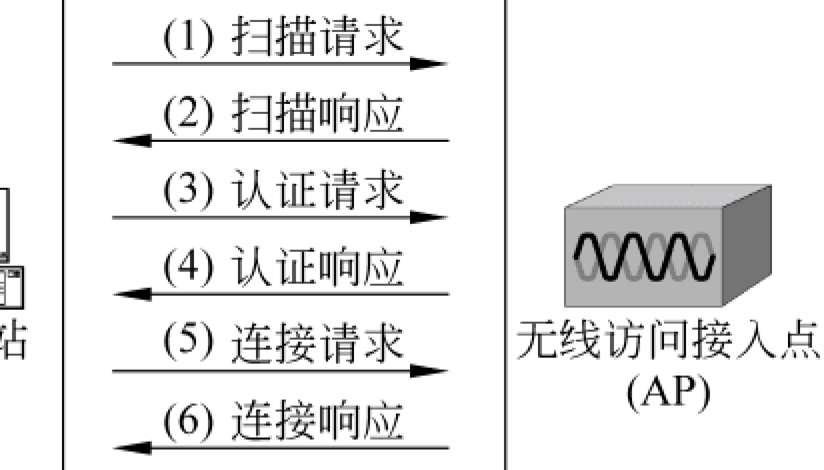



**图 8-7 无线工作站认证**

在图 8-7 中，802.11 客户端的认证有 6 个步骤。

(1) 工作站在每个通道广播扫描请求帧，在一个 WLAN 区域内快速定位某个工作站(通过发送 SSID)。

(2) 在该区域内的 AP 扫描响应帧，这个响应来源于基础结构 BSS 的 AP(对于 IBSS，由响应的工作站发送一个响应帧)。

(3) 工作站确定所需访问的最适合的 AP 发送认证请求。

(4) AP 发送认证响应，在响应中包含用于开放系统的认证算法 ID(对于共享密钥系统，使用 WEP 产生一个随机数和质询文本，包含在响应帧中。这个加密的请求/响应过程未在图中显示，本章后续部分将详细介绍)。

(5) 认证成功后，客户端向 AP 发送连接请求帧，这是一个重要的步骤，保证每个需要向无线工作站发送数据的一方都知道需要通过 AP 发送。

(6) AP 发送连接响应帧。

## 8.2.2 无线局域网的安全缺陷与攻击

在网络中使用无线技术带来了很多的安全问题，网络管理开发需要防止入侵者访问网络，读取或更改网络数据流。解决无线网络安全问题的技术，按开发的时间顺序依次排列为 SSID、开放认证协议和 WEP 协议。WEP 的设计是为了在无线网络中提供类似物理有线网络的安全性。

### 1. SSID 的缺陷

在 AP 的信号帧中，SSID 以明文方式进行广播。虽然信号帧对用户是透明的，但窃听者可以非常方便地使用 802.11 WLAN 嗅探分析器（如 Sniffer Pro、Netstumbler 和 Kismet）来确定 SSID。一些 AP 生产厂家，包括 Cisco 公司，都提供在信号帧中禁止 SSID 广播的选项。但对窃听者来说，仍可通过嗅探到的响应帧来获取 SSID 值。因此，不建议采用 SSID 作为安全手段。

### 2. 开放认证的缺陷

使用开放认证的无线网络存在很大的缺陷，AP 无法确定一个用户是否为合法用户。对于公共的 WLAN 部署，不需要执行很强的访问认证，但需要采用高层的认证。

### 3. 共享密钥认证的缺陷

在深入研究 WEP 的主要缺陷之前，首先详细了解共享密钥的认证过程。

1）WEP 协议概述

WEP 协议主要有保密性、访问控制和数据完整性三个目标。这三个目标的完成，可以协助管理员防止非授权用户使用无线网络或者分析无线数据流。共享密钥认证过程需要客户端配置静态的 WEP 密钥。图 8-8 描述了共享密钥认证过程，步骤如下。

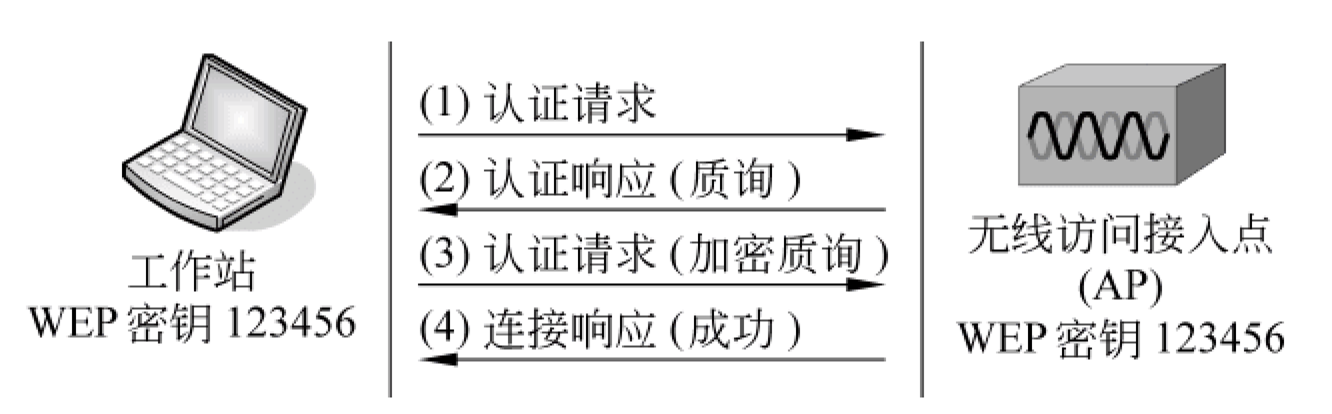



**图 8-8　使用 WEP 的无线工作站认证**

（1）客户端向 AP 发送共享密钥认证请求。

（2）AP 使用 WEP 算法产生一个随机数，包含在认证响应的质询文本中。

（3）客户端使用本地配置的 WEP 密钥加密质询文本，返回一个加密认证请求。

（4）如果可以解密认证请求并获得最初的质询文本，说明客户端通过认证，AP 返回一个认证响应并授权用户访问。

2）WEP 协议的缺陷

从图 8-8 可以发现，交换质询文本的过程是通过无线连接进行的，会被“中间人攻击”（man-in-the-middle attack）所利用。攻击者可以捕获明文（质询文本）以及加密的质询响应。

**注意**：为攻击成功，中间人必须对质询响应解密，从而获得 WEP 密钥。在 2001 年以前 WEPcrack 和 Airsnort 等程序可以识别弱 WEP 密钥和质询，使攻击者的工作变得简单快速。目前，一些厂商修改了产生密钥和质询的硬件，这种现象已经不存在。

图 8-9 描述了中间人攻击。

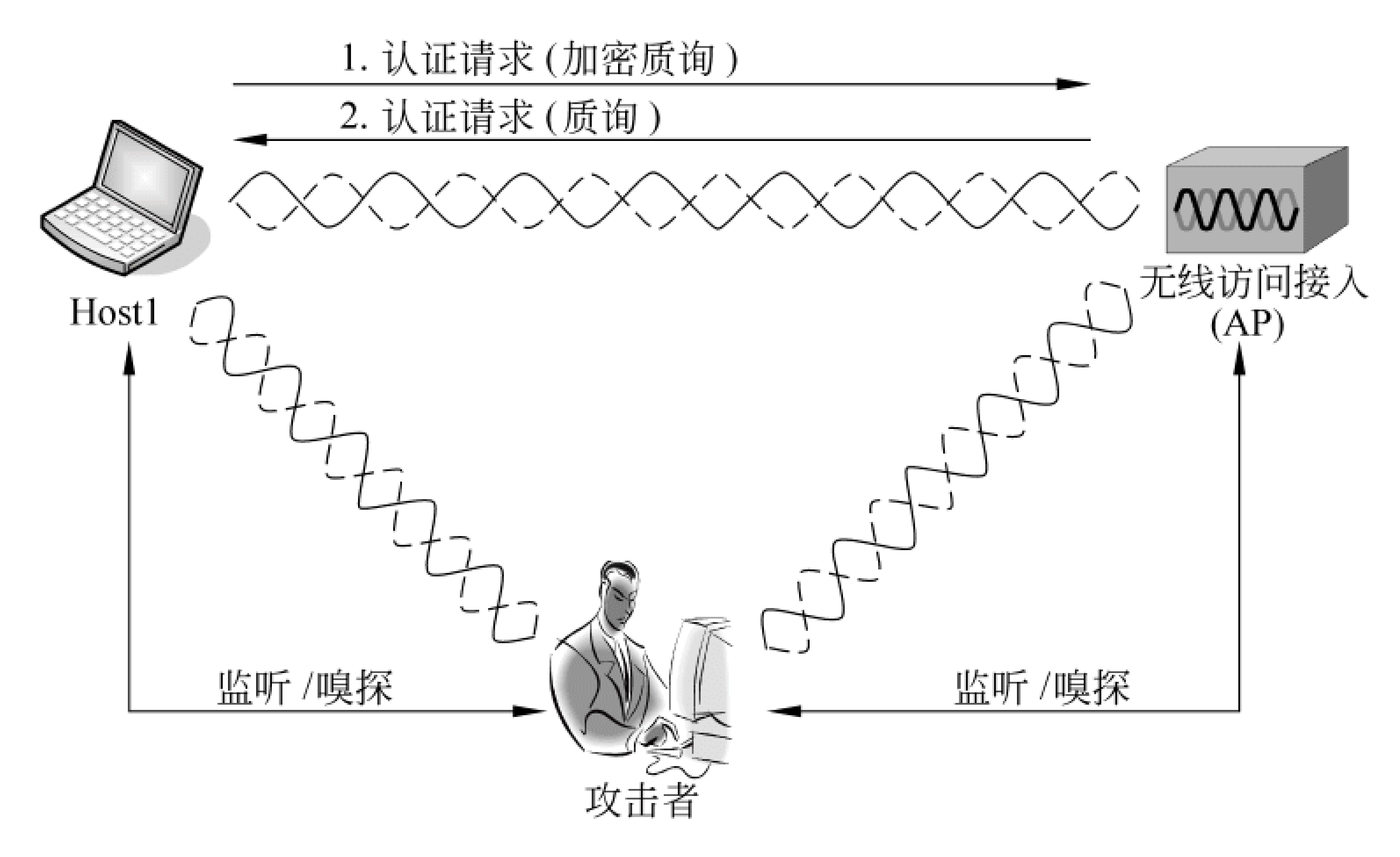



**图 8-9　WEP 的弱点**

WEP 对明文和密钥序列使用异或(XOR)功能产生加密质询。

**注意**：异或(XOR)功能可以描述为，A、B 均为真或 A、B 均为假时，结果为假。当两个输入不同时，XOR 操作的结果为逻辑 1。如果输入相同，结果为逻辑 0。这个功能通常被称为“无进制加法”(add without carry)。

如果对明文和加密质询进行异或操作，得到的结果就是密钥序列。因此，攻击者可以方便地通过协议分析器嗅探共享密钥认证过程计算出密钥序列。很多其他攻击，如消息更改、消息插入和重定向，都是基于这样的入侵技术。

显然，WEP 没有达到其希望解决的安全问题这一目标。因此，对网络管理员来说，需要明确 WEP 是不安全的，把无线网络看作是一个公共网络，把它放在防火墙之外并执行额外的认证手段。VPN、IPSec 和 SSH 等高层软件可以加密所有从客户端应用到服务器端应用的数据，保证事务处理的安全，它们也可以应用到 802.11 无线连接上。

3）针对 WEP 协议缺陷的对策

显然，很多 802.11 网络都采用了 WEP 协议，针对 WEP 协议的主要缺陷，802.11 厂商开发了一些专用解决方案。在 IEEE 802.11i 发布之前，Cisco 公司开发了自主的方案来解决 WEP 协议的缺陷。WEP 协议包含 3 个部分：认证框架；认证算法；数据保密或加密算法。

Cisco 公司无线安全套件所包含的增强功能均优于 WEP 协议各个部分的功能。Cisco 公司无线安全套件采用 IEEE 802.1x 标准作为认证框架和基于用户的认证算法，这个算法称为扩展认证协议(extensible authentication protocol，EAP)，这个算法可以产生动态的 WEP 密钥。Cisco 轻型扩展认证协议(light extensible authentication protocol，LEAP)是 Cisco 的专用认证协议，用于 802.11 WLAN 环境。LEAP 的主要目的是在网络和用户之间进行双向认证保护随机密钥以及用户定义的加密会话密钥，更重要的是，LEAP 与目前广泛采用的网络认证机制(如 RADIUS)兼容。

此外，Cisco 开发了临时密钥完整性协议(temporal key integration protocol，TKIP)以提高 WEP 保密性和加密算法。

### 4. War-Driving 攻击和 War-Chalking 攻击

War-Driving 是一种新的网络攻击方式,攻击者在汽车内或汽车顶上使用天线,天线连接车内的笔记本电脑,然后驾车行进(或者有时也停在车库)在电脑上使用特殊的软件记录捕获到的无线网络数据。这种软件可以记录汽车所在位置的经度纬度以及无线网络的信号强度和网络名称。

对于 WLAN 来说,这意味着给新的网络攻击打开了一个后门。因此,对网络的无线部分进行安全网络审计是非常必要的。不管网络部署了多少防火墙,不恰当的无线配置可能使得攻击者有机会不通过防火墙而获得用户网络的访问。

War-Chalking 用于标明何处提供免费的 Internet 访问。这种方式定义了系列符号,标记在人行道、墙壁、柱子以及其他建筑物上,指示附近可以使用的无线连接,每个符号都代表各无线配置信息用户到达这些标记的位置后使用符号所标明的信息,设置无线网络参数就可以连接 Internet。

### 5. 无线局域网欺诈

无线局域网欺诈(fraud)就是利用默认配置漏洞、加密漏洞、密钥管理漏洞和服务设置标识漏洞等突破身份认证的封锁,假冒合法无线客户端或无线 AP 骗取 WLAN 的信任,窃听重要机密信息或非法访问网络资源的攻击行为。实现欺诈的关键是突破身份认证,而通过身份认证最简便的办法就是设法获得 SSID 和 WEP 共享密钥。如前 SSID 漏洞所述,获取 SSID 并不困难,窃取或破译共享密钥才是 WLAN 欺诈的关键要素。

除了使用众多免费的 WEP 共享密钥破译软件之外,由于 WEP 共享密钥认证过程相对简单,通过伪造合法的共享密钥认证过程,仍然有可能实现欺诈意图。在共享密钥认证方式下无线 AP 收到认证请求后,以明文形式发送一个 128 位的随机认证消息,随机认证消息由共享密钥和初始向量通过 RC4 加密算法生成,无线客户端用共享密钥对随机认证消息加密后回送给无线 AP。如果能够积累大量回送给无线 AP 的加密随机认证报文,就有可能破译出无线客户端对明文流加密使用的密钥流,因为加密随机认证报文中隐藏了密钥流。一旦窃听到发送给客户端的明文随机认证响应,就可以用密钥流伪造一个合法的加密随机认证报文,无线 AP 必然错误地认为这是一个合法的无线客户端,共享密钥。认证欺诈过程如图 8-10 所示。

将 SSID、MAC 地址过滤和 WEP 共享密钥多种安全机制组合起来,能够在很大程度上降低安全威胁,多数无线 AP 在开放系统认证、封闭系统认证和共享密钥认证方式下都支持 MAC 地址过滤。如果在封闭系统认证方式下配置了 MAC 地址过滤,无线客户端不仅要向无线 AP 出示正确的 SSID,还需要提交合法的 MAC 地址。

尽管 MAC 地址过滤机制增强了 WLAN 的安全性,但也为无线局域网欺诈提供了机会。由于无线客户端以明文方式向无线 AP 发送 MAC 地址连接请求,利用无线局域网监听工具很容易窃取 WLAN 中其他无线客户端向无线 AP 发送的合法 MAC 地址。此外如果能知道无线客户端使用的无线网络适配器生产厂商,破译 MAC 地址要比破译 WEP 共享密钥容易得多,因为 MAC 地址是通过标准化生成的,通过伪造合法 MAC 地

址就可实现无线局域网欺诈。操作系统和无线网络适配器支持 MAC 地址重新配置功能，也为 MAC 地址欺诈提供了方便。封闭系统认证 MAC 地址欺诈过程如图 8-11 所示。如果伪造 MAC 地址的无线客户端和合法 MAC 地址的无线客户端同时在线，必然会破坏 ARP 缓存表。所以利用 MAC 地址欺诈接入 WLAN 之前，需要用 WLAN 监听工具确认合法 MAC 地址是否在线。




**图 8-10 共享密钥认证欺诈过程**　　**图 8-11 封闭系统认证 MAC 地址欺诈过程**

### 6. 无线 AP 欺诈

无线 AP 欺诈(rogue)是指在 WLAN 覆盖范围内秘密安装无线 AP，窃取通信、WEP 共享密钥、SSID、MAC 地址、认证请求和随机认证响应等保密信息的恶意行为。事实上 WLAN 固有的性质不仅为无线局域网欺诈提供了方便，也为在 WLAN 附近安装欺诈无线 AP 提供了便利条件。

为了实现无线 AP 欺诈目的，需要首先利用 Netstumblor 等 WLAN 探测和定位软件，获得合法无线 AP 的 SSID、信号强度、是否加密等信息。根据信号强度能够将欺诈无线 AP 秘密安装到合适位置，确保无线客户端可以在合法 AP 和欺诈 AP 之间切换，自然还需要将欺诈 AP 的 SSID 设置成合法无线 AP 的 SSID 值。如果 WLAN 采用开放系统认证或封闭系统认证无线 AP 欺诈已经成功。如果 WLAN 采用共享密钥认证，还需要设法获得 WEP 共享密钥才能欺诈成功。

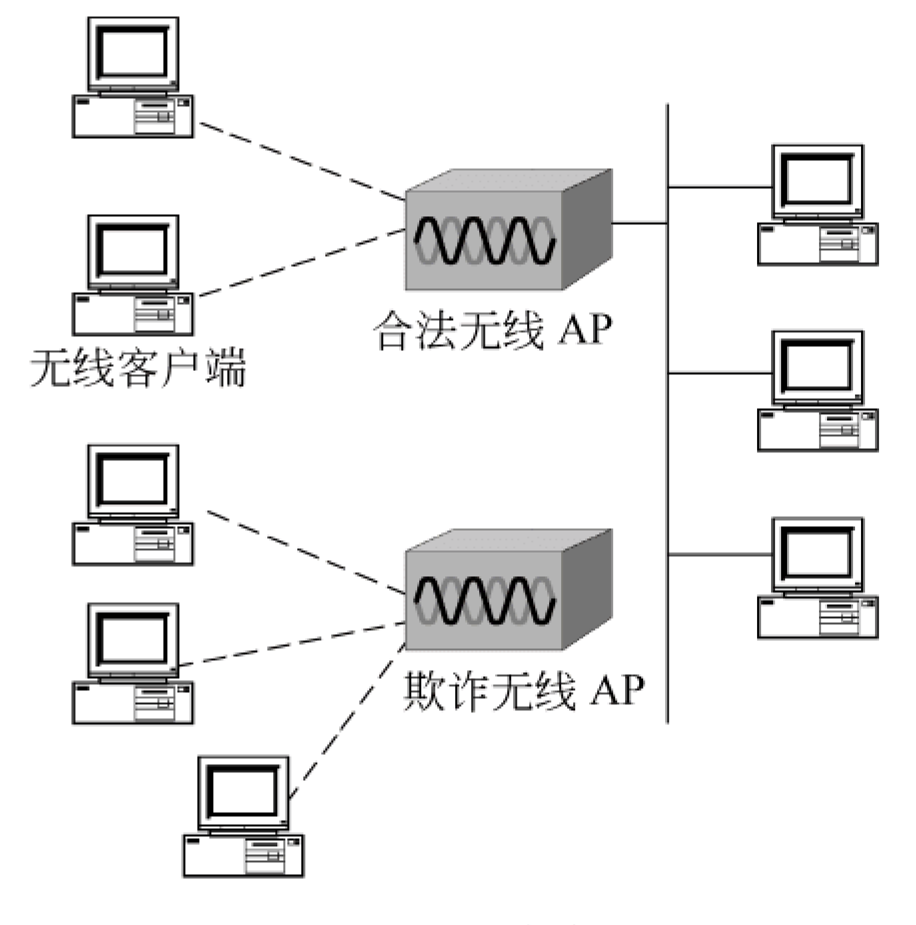



**图 8-12 WLAN 欺诈无线 AP**

发现欺诈无线 AP 最简单的方法就是使用无线局域网探测软件，因为无线局域网探测软件的基本功能就是试图发现非法无线 AP，但前提是欺诈无线 AP 采用了开放系统认证，因为在封闭系统认证或共享密钥认证方式下，无线 AP 并不广播自己的 SSID。WLAN 欺诈无线 AP 如图 8-12 所示。

### 7. 无线局域网劫持

无线局域网劫持(hijack)是指通过伪造 ARP 缓存表使会话流向指定恶意无线客户端的攻击行为，无线局域网劫持原理与有线网络的会话劫持相同，主要是利用了 ARP 协

议中存在的请求与应答报文漏洞。

最初在设计 ARP 协议时没有考虑 ARP 发送请求进程与侦听应答进程之间的关联，换句话说，发送主机接收到 ARP 应答报文时，并不清楚是否曾发送过 ARP 请求报文。主机只要接收到 ARP 应答报文，就将 MAC 地址保存到 ARP 缓存表中。正是 ARP 发送请求进程与侦听应答进程之间的无关联性，为通过伪造 MAC 地址实现会话劫待提供了机会。

同一网段及不同网段内的无线局域网劫持过程如图 8-13 所示。假设恶意无线客户端的 IP 地址和 MAC 地址分别为 192.168.0.1 和 00-00-86-01-02-0B，路由器的 IP 地址和 MAC 地址分别为 192.168.0.3 和 00-00-86-01-02-0D。如果恶意无线客户端希望劫持同一网段内 IP 地址为 192.168.0.0 的无线客户端会话，只要恶意无线客户端知道对方的 IP 地址，并向其发送一个包含自己 MAC 地址 00-00-86-01-02-0B 的 ARP 应答报文。无线客户端将错误地认为 00-00-86-01-02-0B 就是目标主机的 MAC 地址，此时无线客户端的所有报文将被劫持到恶意无线客户端。如果恶意无线客户端希望劫持位于另一网段内 IP 地址为 192.168.0.2 的无线客户端会话，则必须向路由器发送伪造的 MAC 地址 00-00-86-01-02-0B 使路由器 ARP 缓存表错误地将无线客户端的 IP 地址 192.168.0.2 映射成 00-00-86-01-02-0B，路由器会将无线客户端发送的所有报文错误地转发到恶意无线客户端。

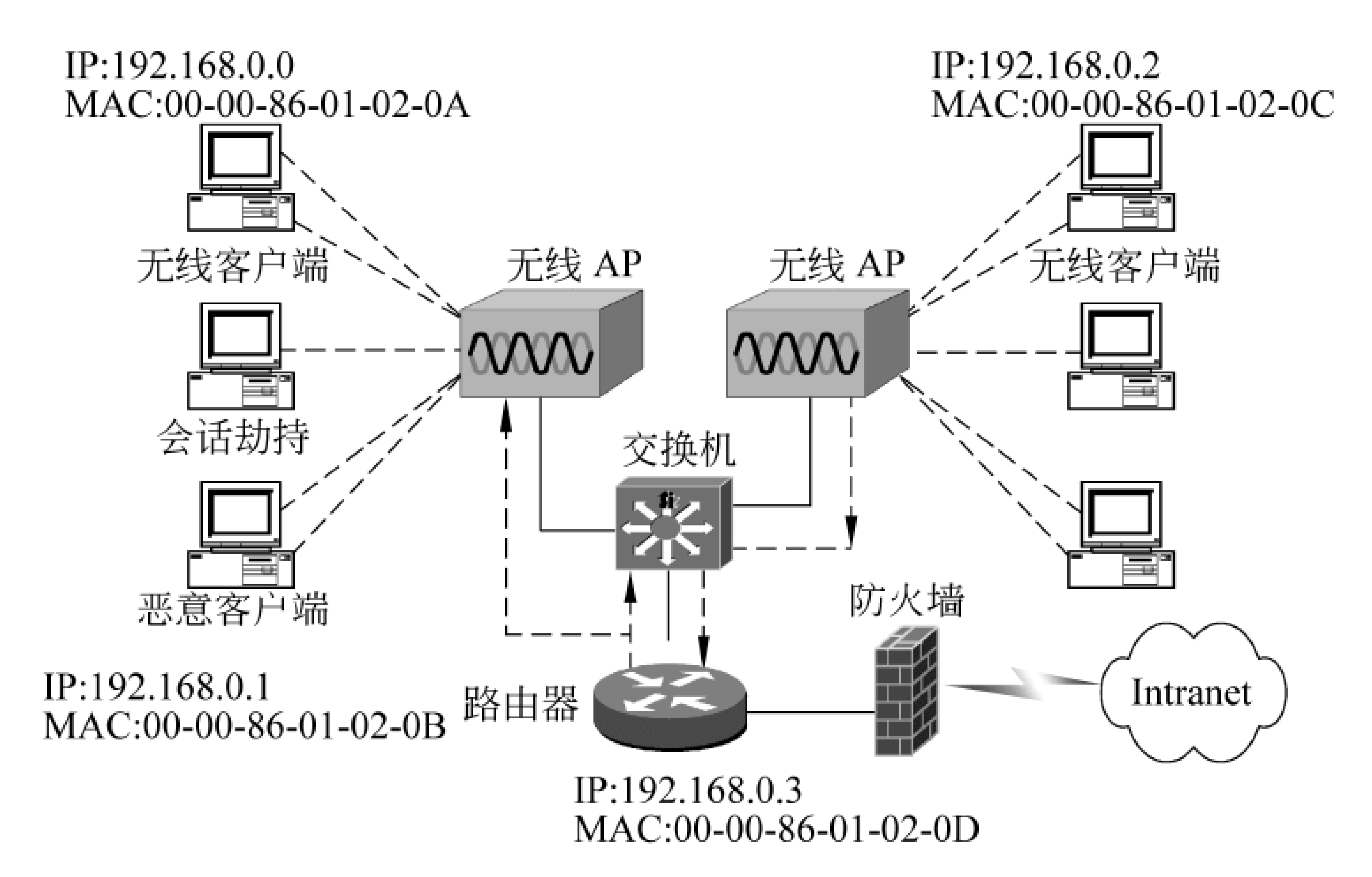



**图 8-13 同一网段及不同网段 WLAN 劫持过程**

目前网络上存在大量免费的会话劫持软件，甚至有些劫持软件还提供源代码，只要在搜索引擎中输入关键词 ARP Spoof 就可以发现众多的劫持软件。例如，Dsniffer、Bktspibdc、WCI、ARP0C2、Hunt、Fake、ARPtool 等都是典型的 ARP 会话劫持软件。从无线局域网会话劫持的原理可以看出，能够实现会话劫持的前提是 ARP 协议使用了动态绑定机制。因此，只要采用静态 ARP 缓存表就可以有效地防止这种会话劫持攻击，但手工维护大量的静态 MAC 地址会给安全管理增加额外的维护负担。

**8. EAP 协议和 802.11i 标准**

802.1x 认证框架包含在 802.11i 标准的 MAC 层安全性增强草案中。802.1x 框架为链路层提供了扩展的认证能力，可以由高层协议调用。EAP 是一种高层协议，是 Cisco 公司的专有协议。网络层协议在链路上传输之前，WEP 允许和认证对端协商认证协议。图 8-14 说明了这些层次之间的关系。

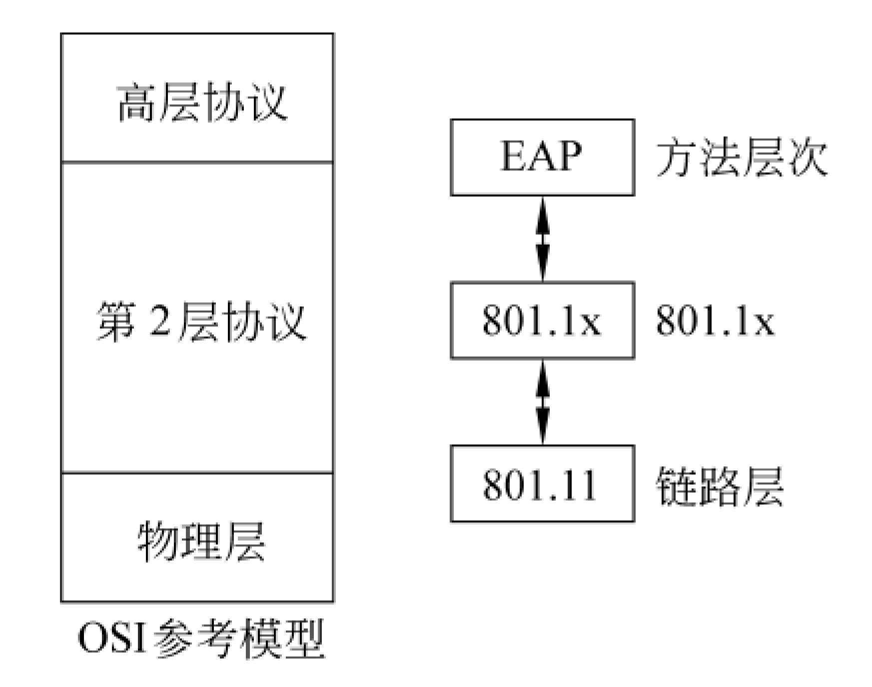



**图 8-14 802.1x 认证框架**

EAP 在 RFC 2284 中定义用于提供强健的、易部署和易于管理的无线安全。Cisco 公司提供对第三方 NIC 以及 RADIUS 支持，使得用户可以使用现有的无线网络投资。图 8-15 说明了使用 EAP 协议和 RADIUS 进行认证的过程。

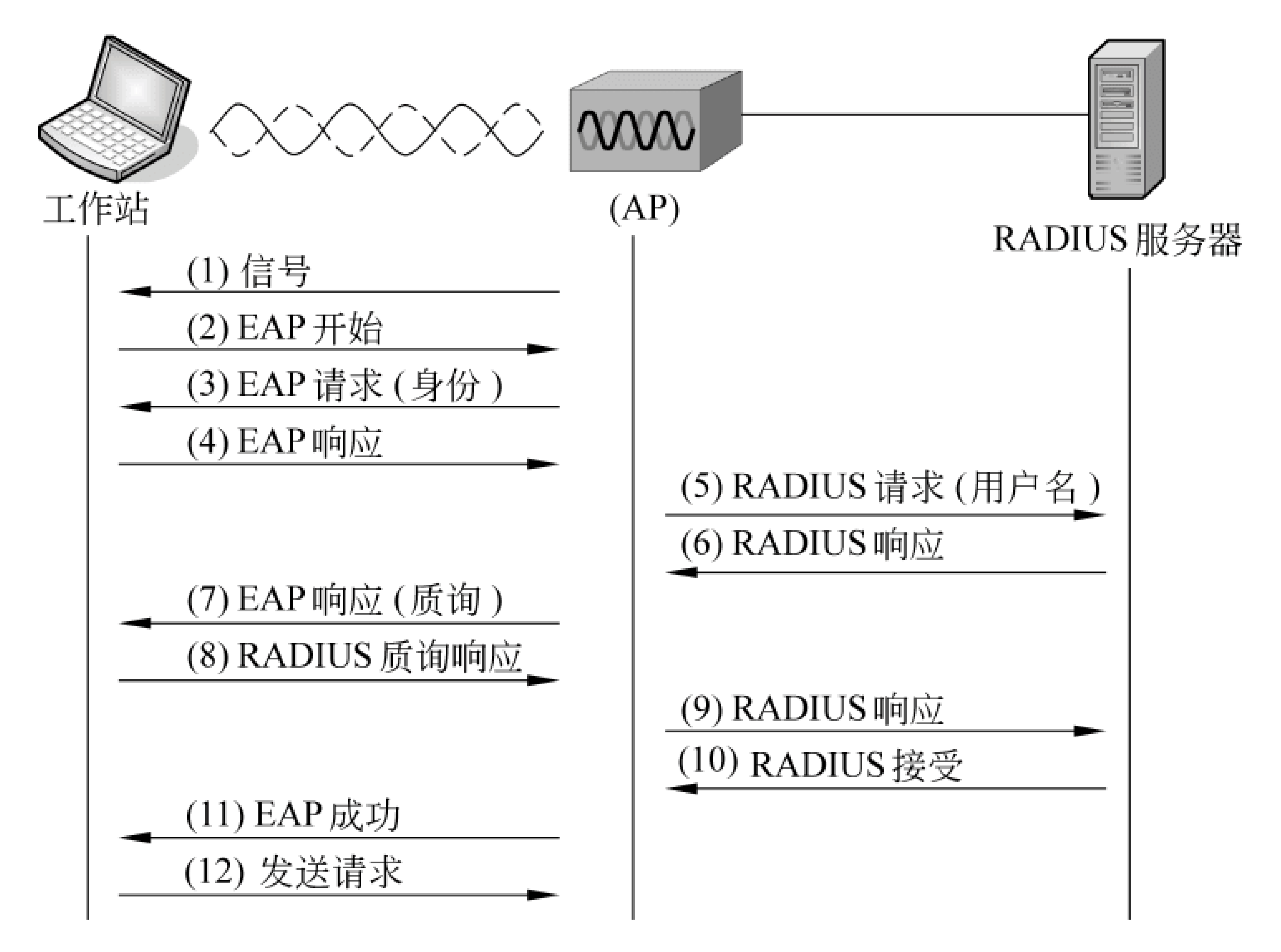



**图 8-15 采用 RADIUS 的认证框架**

从图 8-15 中可知，认证过程由多个步骤构成。

(1) 无线工作站确定从 AP 发出的信号中支持 802.11i。

(2) 工作站使用 EAP 帧开始会话。

(3) AP 向工作站发送 EAP 身份请求消息。

(4) 工作站发送 EAP 响应(其中包含工作站 ID)。

(5) AP 向 RADIUS 服务器转发数据分组(含工作站 ID)。

(6) RADIUS 向 AP 发送响应，其中包含质询(EAP 认证类型)。

(7) AP 向工作站转发质询。

(8) 工作站发送质询响应(含 EAP 类型)。

(9) AP 向 RADIUS 服务器转发响应。

(10) RADIUS 服务器向 AP 发送接受消息。

(11) AP 向工作站转发 EAP 成功消息。

(12) 工作站准备数据传输。

此时建议可采用 VPN、IPSec、SSH 等加密客户端和服务器端所有数据的机制可以为 EAP 提供更强的事务安全性,这些机制又增加了一个安全层次。

网络管理员必须尽可能地保证 WLAN 部署的安全,明确 802.11 标准的安全缺陷。采用 Cisco 无线安全套件可以增强安全性,有助于建立安全的 WLAN。

### 8.2.3 无线局域网安全解决方案

合理保护无线访问点的目的在于,将无线网络与无权使用服务的外人隔离开来。就安全而言,无线网络通常比固定有线网络更难保护,这是因为有线网络的固定物理访问点数量有限,而在天线辐射范围内的任何一点都可以使用无线网络。尽管本身存在着困难,但合理保护无线网络系统是保护系统避免严重安全问题的关键所在。

#### 1. 无线局域网安全策略

在使用了 802.1x、EAP、AES 和 TKIP 之后,还需要了解其中的一些问题,这些是建立安全 WLAN 网络环境必需的。首先,IEEE 802.11i 工作小组所建立的 TKIP,是为了快速修正 WEP 的严重问题。TKIP 在算法上与 WEP 相同,也是使用 RC4 算法,但这种算法并不是最理想的选择。使用 AES 能把原来的问题解决得更好,但是 AES 无法与原有的 802.11 架构兼容,需要升级软硬件。第二,一些新的协议、技术的加入,与原有 802.11 混合在一起,使得整个网络结构更加复杂,同时也增加了处理的负担,导致网络性能降低。新的技术让生产厂商和网络用户有更多的可选择性,但同时也带来了兼容性的问题。第三,对于用户来说,在购买设备之前,需要了解产品能提供什么样的功能,有什么样的兼容性的要求。例如,从公司 A 购买了 AP,然后从公司 B 和公司 C 购买了无线网卡,很可能存在因兼容性导致某些功能无法使用的问题。

从企业角度而言,随着无线网络应用的推进,企业需要更加注重无线网络安全的问题,针对不同的用户需求,提出一系列不同级别的无线安全技术策略。从传统的 WEP 加密到 IEEE 802.11i,从 MAC 地址过滤到 IEEE 802.1x 安全认证技术,要分别考虑能满足单一的家庭用户、大中型企业、运营商等不同级别的安全需求。

对于小型企业和家庭用户而言,无线接入用户数量比较少,一般没有专业的 IT 管理人员,对网络安全性的要求相对较低。通常情况下不会配备专用的认证服务器,这种情况下,可直接采用 AP 进行认证,WPA-PSK+接入点隐藏可以保证基本的安全级别。

在仓库物流、医院、学校等环境中,考虑到网络覆盖范围以及终端用户数量,AP 和无线网卡的数量必将大大增加,同时由于使用的用户较多,安全隐患也相应增加,此时简单的 WPA-PSK+已经不能满足此类用户的需求。如表 8-3 中所示的中级安全方案使用支持 IEEE 802.1x 认证技术的 AP 作为无线网络的安全核心,并通过后台的 RADIUS 服务器进行用户身份验证,有效地阻止未经授权的用户接入。

在各类公共场合以及网络运营商、大中型企业、金融机构等环境中,有些用户需要在

热点公共地区(如机场、咖啡店等)通过无线接入 Internet,因此用户认证问题就显得至关重要。如果不能准确可靠地进行用户认证,就有可能造成服务盗用的问题,这种服务盗用对于无线接入服务提供商来说是不可接受的损失,表 8-3 中专业级解决方案可以较好地满足用户需求,通过用户隔离技术、IEEE 802.1i、RADIUS 的用户认证以及计费方式确保用户的安全。

如表 8-3 所示,目前采用 WLAN 可以部署三种不同级别的 WLAN 安全措施:基本安全、增强安全和专业安全。像所有其他有关安全的部署一样,在选择和部署任何一种 WLAN 安全解决方案之前先进行网络风险评估。

**表 8-3 三种无线网络安全级别比较**

| 安全级别 | 典型场合 | 使用技术 |
| --- | --- | --- |
| 基本安全 | 小型企业,家庭用户等 | WPA-PSK+接入点隐藏 |
| 增强安全 | 仓库物流、医院、学校、餐饮娱乐 | IEEE 802.1x 认证+TKIP 加密 |
| 专业级安全 | 各类公共场合及网络运营商、大中型企业、金融机构 | 用户隔离技术+IEEE 802.11i+RADIUS 认证和计费(对运营商) |

### 2. 增强安全解决方案

增强安全解决方案利用针对每个用户、每个会话的动态 WEP 密钥来阻止未经授权的网络访问。该解决方案建立在 802.1x 身份认证框架和 EAP 的基础之上,可以提供基于用户的身份认证。它弥补了第一代静态 WEP 密钥和基本安全保护的所有不足。

部署大规模的企业 WLAN,网络管理员需要可扩展的、轻松的管理方案,以避免加重人员的工作负担。增强的安全保护可以提供一个这样的解决方案,同时还可以阻止各种精心策划的被动或者主动的 WLAN 攻击,消除对于管理静态 WEP 密钥的需要。这种强大的企业级 WLAN 安全解决方案可以将服务质量和移动性集成到它的框架之中,从而可以支持一组更加丰富的企业级应用。

思科的无线安全套件采用了一种增强的安全解决方案。思科扩展了 EAP,创建了 Cisco LEAP,它也被称为 EAP Cisco Wireless。思科无线安全套件的企业级安全架构包括双向身份认证、消息完整性检查(MIC)、逐个分组密钥散列、基于策略的密钥旋转、初始化向量(VI)变化以及远程拨号用户认证服务(RADIUS)记账记录的可用性。

### 3. 专业安全解决方案

在某些情况下,企业可能需要端到端的安全性来保护他们的业务应用。管理员可以利用专业安全保护建立一个虚拟专用网(VPN),让身处公共场所(例如机场和宾馆)的移动用户可以通过隧道访问企业网络。为了建立一个安全的 VPN,管理员必须特别注意隧道、加密、分组完整性、防火墙、用户和设备认证以及网络管理等。这个解决方案需要一个 VPN 终端。

大多数用户都不需要在他们的内联网中部署一个专业安全 WLAN。有些特殊行业,例如需要采取广泛的安全措施的金融机构,可能需要部署专业安全解决方案和增强的安

全方案。但是对于绝大多数用户的网络来说,思科无线安全套件所提供的安全更加适用,因为它可以避免建立 VPN 所需要的开支和费用。

1) 思科解决方案概述

思科的 SAFE 蓝图可以利用 EAP Cisco Wireless 和 VPN 部署一个专业安全解决方案的网络设计人员提供指导。SAFE 蓝图是一种模块化的方法,可以有效地保障那些指定了安全设计、部署和管理流程的 WLAN 网络的安全。图 8-16 是利用思科无线安全套件实现 EAP Cisco Wireless 双向认证和集中式 WEP 密钥管理的构架。

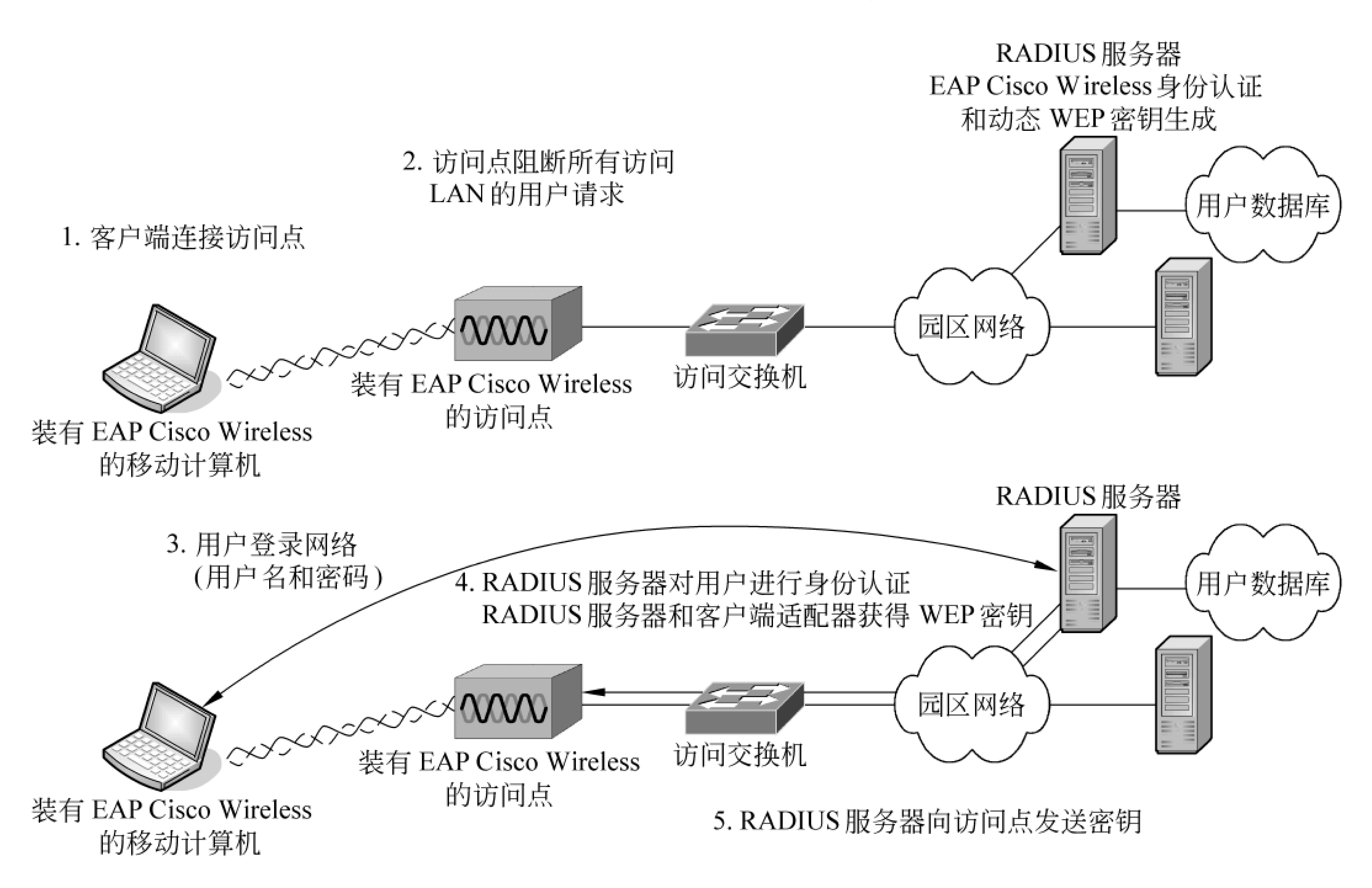



**图 8-16 思科无线安全解决方案**

利用双向认证和动态 WEP 密钥,新的思科无线安全套件为企业局域网管理员们提供了将无线技术引入网络所需要的信心。它的高度的灵活性使网络管理人员可以自行选择自己需要的保护等级,并且非常牢固,足以提供一个安全框架,并围绕这个框架建立整个安全解决方案。它的安全管理非常方便,因而不会加重 IT 人员的管理负担。

一个用户要想安全地连接到思科无线安全套件只需要一个 Cisco Aironet 系列 WLAN 客户端适配器(访问卡),启用了安全特性的新型 Cisco Aironet 客户端工具(ACU)以及针对特定的覆盖区域的服务集标识符(SSID)。WLAN 基础设施包括一个运行着思科无线安全套件的 Cisco Aironet 系列访问点和一个认证、授权和记账(AAA)RADIUS 服务器。只需单击一个按钮,文件就可以从员工的计算机,通过 Cisco Aironet WLAN 客户端适配器发送到运行着思科无线安全套件并连接到 RADIUS 服务器的 Cisco Aironet 访问点。整个过程没有任何不便,非常安全。

思科无线安全套件的另外一个附加特性是能够为每个客户端进程生成详细的RADIUS记账记录。这些记录可以被发送到AAA服务器,用于记录、审计和针对WLAN的使用收取费用。企业还可以利用这些数据审查账目。

利用思科无线安全套件,网络管理人员可以部署一个能够提供强大的企业级WLAN安全的无线解决方案。这个解决方案包括了很多来自于802.11标准的建议,该标准重新定义了WLAN怎样阻止那些对于基于静态WEP的系统来说非常有效的攻击。

思科的客户端适配器和访问点拥有各种支持动态WEP密钥生成、双向认证的增强特性,以及思科无线安全套件的其他一些优点。在采用了思科基础设施、客户端卡、固件/驱动器/工具和RADIUS服务器,并且启用了思科无线安全套件以后,就可以全面实施下列安全措施。

利用Cisco Aironet的密钥旋转系统,WLAN可以支持针对用户、针对会话的密钥和广播密钥。单播密钥的重置超时策略在思科安全ACS(基于Windows)或者Cisco AR(基于UNIX)集中配置。这个密钥旋转过程对于用户来说是透明的。网络管理人员可以在访问点配置组播密钥旋转策略。

2) EAP Cisco Wireless优点

Cisco Aironet产品支持IEEE 802.1x标准框架和EAP以及EAP认证类型,例如EAP-TLS和EAP Cisco Wireless。与基本的EAP相比,EAP Cisco Wireless具有两个重要的优点。

(1) 客户端和RADIUS服务器之间的双向认证机制,这可以有效地阻止由伪装的访问点发动的“中间人”式攻击。这也有助于确保只有合法的客户端才能连接合法的、经过授权的无线访问点。

(2) 对WLAN的集中式密钥管理。在成功地认证了客户端的身份以后,RADIUS服务器和客户端将获得一个针对用户的WEP密钥,客户端将在本次登录会话中使用这个密钥。

3) 思科无线安全套件的攻击防范

思科解决方案可以阻止各种攻击。该解决方案可以防范AirSnort攻击和强力攻击、通过丢失或者被盗的设备发动的入侵、中间人攻击、利用针对分组的密钥散列阻止“Weak IV”式攻击以及重复攻击。

(1) AirSnort攻击。

思科无线安全套件可以通过提供针对分组的密钥散列以及针对主动的重置密钥的集中式策略配置阻止“Weak IV”式攻击。这些特性可以防止黑客利用“Weak IV”获得足够多的分组以破解密钥。

(2) 强力攻击。

尽管在理论上存在可能性,但是实际上强力攻击非常难以发起,实际上也不会产生任何效果,这要归功于Cisco Aironet针对用户、针对会话的动态WEP密钥和频繁的重置密钥功能。而其他使用基于动态WEP的系统的厂商则很容易受到这种攻击的威胁。

(3) 通过丢失或者被盗的设备发动的攻击。

思科无线安全套件可以最大限度地降低由于损失设备和网络接口卡(NIC)而带来的

风险。在基于 802.1x 的架构中,思科的认证对象是用户,而不是 NIC 卡。

(4) 中间人攻击。

这种攻击可能是主动式或者被动式的。Cisco Aironet 的双向认证机制(EAP Cisco Wireless)可以阻止这种攻击。企业可以放心地部署思科解决方案,而无须担心来自伪装的访问点的威胁。用户密码和会话密钥在无线链路上决不会用明文传送。在这种情况下,无须管理员干预,终端用户就可以自动获得一个独特的会话密钥,从而以一种加密的方式获得对网络的访问。管理员可以通过安排他们的 WLAN,根据他们的需要,每隔一段时间重新进行一次身份认证。

IEEE 802.11 安全任务组(TGi)已经将 802.1x 和 EAP 集成到了它的基本安全框架中。在启用了这些 802.1x 安全特性以后,一个连接到某个访问点的无线客户端只有在用户通过企业 RADIUS 服务器的身份认证以后才能获得对网络的访问权限。

很多第三方 AAA RADIUS 服务器现在也可以支持 Cisco Aironet 安全框架,包括对 EAP Cisco Wireless 双向认证的支持。这些服务器加上思科安全访问控制服务器(ACS)和思科访问注册器(AR),可以帮助网络管理员灵活地选择后端服务,而不需要降低 WLAN 的安全性。

(5) 利用针对分组的密钥散列阻止“Weak IV”式攻击。

思科无线安全套件可以阻止很多类型的攻击,其中包括通过分析一串使用相同密钥的加密流量中的多个不安全的初始化向量而发动的“Weak IV”式攻击。利用客户端和访问点都支持的高级散列技术,WEP 密钥会在每个分组的基础上动态变化,从而有效地阻止这种攻击。IV 和 WEP 密钥都会被散列,以生成一个独特的分组密钥,这可以防止黑客利用不安全的 IV 获得 WEP 密钥。

为了防止利用 IV 冲突而发动的攻击,必须在 IV 发生重复之前更改 IV 密钥。由于在一个繁忙的网络上 IV 可能会几个小时重复出现一次,所以管理员可以利用像 EAP Cisco Wireless 这样的机制进行重置密钥操作。

(6) 重复攻击。

对 WEP 的另外一个担忧是它对重复攻击的抵抗能力。思科无线安全套件可以执行消息完整性检查(MIC)来防止 WEP 帧受到修改。Cisco Aironet WLAN 可以利用 MIC 检测并丢弃那些在传输过程中被(恶意)修改的分组。由于采用了 MIC 的 Cisco Aironet 产品可以利用消息完整性检查发现并丢弃被修改的分组,所以攻击者无法利用位切换或者主动的重复攻击来欺骗网络以通过身份认证。

### 8.2.4 基本安全措施

为了最大限度地堵住这些安全漏洞,对于没有部署整体无线网络安全解决方案的 WLAN,就要确保网络人员采取保护无线网络的以下措施。

#### 1. 规划天线的放置

要部署封闭的无线访问点,第一步就是合理放置访问点的天线,以便能够限制信号在覆盖区以外的传输距离。不要将天线放在窗户附近,因为玻璃无法阻挡信号。你最好

将天线放在需要覆盖的区域的中心,尽量减少信号泄露到墙外。当然,完全控制信号泄露几乎是不可能的,所以还需要采取其他措施(如物理保护)。

### 2. 使用 WEP

在任何可用的地方启用无线加密帧。尽管存在重大缺陷,但 WEP 仍有助于阻挠偶尔闯入的黑客。许多无线访问点厂商为了方便安装产品,交付设备时关闭了 WEP 功能。但一旦采用这做法,黑客就能立即访问无线网络上的流量,因为利用无线嗅探器就可以直接读取数据。

### 3. 变更 SSID 及禁止 SSID 广播

众所周知,服务集标识符(SSID)是无线访问点使用的识别字符串,客户端利用它就能建立连接。该标识符由设备制造商设定,还有一些厂商使用无线网络适配器的半个 MAC 地址作为默认的 SSID,MAC 地址采用十六进制数字表示,长度为 6 个字节。前 3 个字节是 IEEE 分配给厂商的唯一标识编码 OUI(organizationally unique identifier),后 3 个字节为网络适配器的唯一标识编码。表 8-4 是无线 AP 主要厂商默认的 SSID 和 IEEE 分配的 MAC 地址 OUI。

**表 8-4 无线 AP 主要厂商默认的 SSID 和 OUI**

| 厂 商 名 称 | 默认 SSID | OUI |
|---|---|---|
| Cisco | tsunami | 00-40-96 |
| Linksys | linksys | 00-04-5A |
| TP-LINK | Wireless | 00-0A-EB |
| ACCTON | WLAN | 00-00-E8 |
| Compaq | Compaq | 00-02-A5 |
| Intel | Intel,xlan,101 | 00-02-B3 |
| AboveCable | CTC | 00-0D-08 |
| 3Com | 101 | 00-00-86 |
| Dell | Wireless | 00-06-5B |
| SMC Networks | WLAN | 00-04-E2 |
| Aruba | Aruba-AP | 00-0B-86 |

由于同一厂商的 OUI 是完全相同,因此检索或推测出默认的 SSID 并不是一件困难的事。此外,著名的 2600 黑客杂志网站收集了几乎所有厂商的默认 SSI 和 WEP 密钥。倘若黑客知道了这种默认的 SSID,即使未经授权,也很容易使用用户的无线服务。对于部署的每个无线访问点而言,要选择独一无二并且很难猜中的 SSID。如果可能的话,禁止通过天线向外广播该标识符。这样网络仍可使用,但不会出现在可用网络列表上。

### 4. 禁用 DHCP

对无线网络而言,这很有意义。如果采取这项措施,黑客不得不破译 IP 地址、子网掩码及其他所需的 TCP/IP 参数。无论黑客怎样利用访问点,仍需要弄清楚 IP 地址。

### 5. 禁用或改动 SNMP 设置

如果访问点支持 SNMP,要么禁用,要么改变公开及专用的共用字符串,并且采用只读方式。如果不采取这项措施,黑客就能利用 SNMP 获得有关你方网络的重要信息。

### 6. 使用访问列表

为了进一步保护无线网络,如果可能的话请使用访问列表。不是所有的无线访问点都支持这项特性,但如果网络支持,就可以具体地指定允许哪些机器连接到访问点。支持这项特性的访问点有时会使用普通文件传输协议(TFTP),定期下载更新的列表,以避免管理员必须在每台设备上使这些列表保持同步的棘手问题。

## 8.3 网络安全解决实例

从目前网络安全厂商所提供的安全解决方案来看,现有解决方案具有以下特征。

### 1. 解决方案的整体性

现有解决方案基本上融合了防/杀病毒、防火墙、信息加密、安全认证以及入侵检测和网络安全评估等全线安全产品和服务,在此基础上有些厂商还加入了自己开发的数据恢复功能。

### 2. 构建基于企业自身的核心产品和技术

为了突出自身产品的价值和地位,现有解决方案提供商基本上是以自有产品作为解决方案的核心,而把其他厂商的产品作为解决方案必不可少的组成部分。

### 3. 集中于特定行业

现有网络安全解决方案所面向的行业主要集中于金融、证券、电信和政府部门,有些厂商还提出了面向城域网的安全解决方案,而面向广大中小企业级的解决方案则相对较少。

### 4. 安全服务已成为解决方案的重要组成部分

在现有网络安全解决方案中,有相当数量的厂商都已经把提供安全服务作为解决方案的一部分。现有安全服务包括两种形式:一是作为产品形式而存在的服务,如网络安全评估、系统安全评估等;二是专业化的服务,包括系统设计、用户培训、系统实施、系统维护等。为用户提供全面的安全服务已成为安全产品厂商拓展市场,取得可持续发展的

重要赢利模式之一。

## 8.3.1 校园网安全解决方案

校园网已成为各高等院校信息技术的基础设施，是学校可持续发展的重要保证。校园网总体上分为校园内网和校园外网。校园内网主要包括教学局域网、图书馆局域网、办公自动化局域网等。校园外网主要指学校提供对外服务的服务器群、与 Internet 的接入以及远程移动办公用户的接入等。校园网的服务器群构成了校园网的服务系统，主要包括 DNS、Web、FTP、MAIL、视频点播、教学平台等。外部网实现了校园网与 Internet 的基础接入，使院校教员和学生能使用电子邮件和浏览器等应用方式，在教学、科研和管理工作中利用国内和国际网进行信息交流和共享。校园网是校内外信息交流的窗口，也是高校教学、科研和行政管理不可缺少的重要基础设施。校园网结构开放，同时与教育网和 Internet 相连接。近年来，随着学生宿舍、教职工家属等接入校园网后，网络规模急剧增大，校园网用户组成复杂，用户水平参差不齐，其中不乏技术高超的黑客，这些因素使校园网的维护和管理变得十分困难。同时，校园网络的应用水平也在不断提高。规模的壮大和运用水平的提高就决定了校园网面临的隐患也相应加剧。由此可见，构筑网络安全防御体系是非常必要的。

### 1. 校园网安全隐患分析

当前校园网络存在的安全隐患和漏洞有如下几点。

(1) 校园网通过 CERNET 与 Internet 相连，在享受 Internet 方便快捷的同时，也面临着遭遇攻击的风险。即使有防火墙的保护，由于技术本身的局限或错误配置等原因，仍很难保证校园网不遭到黑客攻击。

(2) 校园网内部也存在很大的安全隐患，网络设备包括服务器、交换机、集线器、路由器、工作站、电源等分布在整个校园内，管理起来非常困难。由于内部用户对网络的结构和应用模式都比较了解，因此来自内部的安全威胁更大一些。现在，黑客攻击工具在网上泛滥成灾，大学生的好奇心理较强，决定了其利用这些工具进行攻击的可能性。部分学生可能出于各种目的在内部进行恶意操作，有意或无意地将它们损坏，经常会引发内部校园网安全危机，往往会造成校园网络全部或部分瘫痪。

(3) 目前网络服务器安装的操作系统有 Windows NT/Windows 2000、UNIX、Linux 等，这些系统安全风险级别不同，例如 Windows NT/Windows 2000 的普遍性和可操作性使得它也是最不安全的系统；UNIX 由于其技术的复杂性导致高级黑客对其进行攻击，这都对原有网络安全构成威胁。

(4) 随着校园内计算机应用的大范围普及，接入校园网节点日渐增多，而这些节点大部分都没有采取一定的防护措施，随时有可能造成病毒泛滥、信息丢失、数据损坏、网络被攻击、系统瘫痪等严重后果。例如，一些只对校园内部用户开放的服务，常常被设置后门。比较典型的例子，高校数字图书馆通常都限定只对内部 IP 开放，然而有的学生会在校内安置代理程序，供外部人员访问，造成学校信息的泄露。

(5) 内部用户对 Internet 的非法访问威胁，如浏览黄色、暴力、反动等网站，以及由于

重要赢利模式之一。

## 8.3.1 校园网安全解决方案

校园网已成为各高等院校信息技术的基础设施,是学校可持续发展的重要保证。校园网总体上分为校园内网和校园外网。校园内网主要包括教学局域网、图书馆局域网、办公自动化局域网等。校园外网主要指学校提供对外服务的服务器群、与 Internet 的接入以及远程移动办公用户的接入等。校园网的服务器群构成了校园网的服务系统,主要包括 DNS、Web、FTP、MAIL、视频点播、教学平台等。外部网实现了校园网与 Internet 的基础接入,使院校教员和学生能使用电子邮件和浏览器等应用方式,在教学、科研和管理工作中利用国内和国际网进行信息交流和共享。校园网是校内外信息交流的窗口,也是高校教学、科研和行政管理不可缺少的重要基础设施。校园网结构开放,同时与教育网和 Internet 相连接。近年来,随着学生宿舍、教职工家属等接入校园网后,网络规模急剧增大,校园网用户组成复杂,用户水平参差不齐,其中不乏技术高超的黑客,这些因素使校园网的维护和管理变得十分困难。同时,校园网络的应用水平也在不断提高。规模的壮大和运用水平的提高就决定了校园网面临的隐患也相应加剧。由此可见,构筑网络安全防御体系是非常必要的。

### 1. 校园网安全隐患分析

当前校园网络存在的安全隐患和漏洞有如下几点。

(1) 校园网通过 CERNET 与 Internet 相连,在享受 Internet 方便快捷的同时,也面临着遭遇攻击的风险。即使有防火墙的保护,由于技术本身的局限或错误配置等原因,仍很难保证校园网不遭到黑客攻击。

(2) 校园网内部也存在很大的安全隐患,网络设备包括服务器、交换机、集线器、路由器、工作站、电源等分布在整个校园内,管理起来非常困难。由于内部用户对网络的结构和应用模式都比较了解,因此来自内部的安全威胁更大一些。现在,黑客攻击工具在网上泛滥成灾,大学生的好奇心理较强,决定了其利用这些工具进行攻击的可能性。部分学生可能出于各种目的在内部进行恶意操作,有意或无意地将它们损坏,经常会引发内部校园网安全危机,往往会造成校园网络全部或部分瘫痪。

(3) 目前网络服务器安装的操作系统有 Windows NT/Windows 2000、UNIX、Linux 等,这些系统安全风险级别不同,例如 Windows NT/Windows 2000 的普遍性和可操作性使得它也是最不安全的系统;UNIX 由于其技术的复杂性导致高级黑客对其进行攻击,这都对原有网络安全构成威胁。

(4) 随着校园内计算机应用的大范围普及,接入校园网节点日渐增多,而这些节点大部分都没有采取一定的防护措施,随时有可能造成病毒泛滥、信息丢失、数据损坏、网络被攻击、系统瘫痪等严重后果。例如,一些只对校园内部用户开放的服务,常常被设置后门。比较典型的例子,高校数字图书馆通常都限定只对内部 IP 开放,然而有的学生会在校内安置代理程序,供外部人员访问,造成学校信息的泄露。

(5) 内部用户对 Internet 的非法访问威胁,如浏览黄色、暴力、反动等网站,以及由于

重要赢利模式之一。

### 8.3.1 校园网安全解决方案

校园网已成为各高等院校信息技术的基础设施,是学校可持续发展的重要保证。校园网总体上分为校园内网和校园外网。校园内网主要包括教学局域网、图书馆局域网、办公自动化局域网等。校园外网主要指学校提供对外服务的服务器群、与 Internet 的接入以及远程移动办公用户的接入等。校园网的服务器群构成了校园网的服务系统,主要包括 DNS、Web、FTP、MAIL、视频点播、教学平台等。外部网实现了校园网与 Internet 的基础接入,使院校教员和学生能使用电子邮件和浏览器等应用方式,在教学、科研和管理工作中利用国内和国际网进行信息交流和共享。校园网是校内外信息交流的窗口,也是高校教学、科研和行政管理不可缺少的重要基础设施。校园网结构开放,同时与教育网和 Internet 相连接。近年来,随着学生宿舍、教职工家属等接入校园网后,网络规模急剧增大,校园网用户组成复杂,用户水平参差不齐,其中不乏技术高超的黑客,这些因素使校园网的维护和管理变得十分困难。同时,校园网络的应用水平也在不断提高。规模的壮大和运用水平的提高就决定了校园网面临的隐患也相应加剧。由此可见,构筑网络安全防御体系是非常必要的。

**1. 校园网安全隐患分析**

当前校园网络存在的安全隐患和漏洞有如下几点。

(1) 校园网通过 CERNET 与 Internet 相连,在享受 Internet 方便快捷的同时,也面临着遭遇攻击的风险。即使有防火墙的保护,由于技术本身的局限或错误配置等原因,仍很难保证校园网不遭到黑客攻击。

(2) 校园网内部也存在很大的安全隐患,网络设备包括服务器、交换机、集线器、路由器、工作站、电源等分布在整个校园内,管理起来非常困难。由于内部用户对网络的结构和应用模式都比较了解,因此来自内部的安全威胁更大一些。现在,黑客攻击工具在网上泛滥成灾,大学生的好奇心理较强,决定了其利用这些工具进行攻击的可能性。部分学生可能出于各种目的在内部进行恶意操作,有意或无意地将它们损坏,经常会引发内部校园网安全危机,往往会造成校园网络全部或部分瘫痪。

(3) 目前网络服务器安装的操作系统有 Windows NT/Windows 2000、UNIX、Linux 等,这些系统安全风险级别不同,例如 Windows NT/Windows 2000 的普遍性和可操作性使得它也是最不安全的系统;UNIX 由于其技术的复杂性导致高级黑客对其进行攻击,这都对原有网络安全构成威胁。

(4) 随着校园内计算机应用的大范围普及,接入校园网节点日渐增多,而这些节点大部分都没有采取一定的防护措施,随时有可能造成病毒泛滥、信息丢失、数据损坏、网络被攻击、系统瘫痪等严重后果。例如,一些只对校园内部用户开放的服务,常常被设置后门。比较典型的例子,高校数字图书馆通常都限定只对内部 IP 开放,然而有的学生会在校内安置代理程序,供外部人员访问,造成学校信息的泄露。

(5) 内部用户对 Internet 的非法访问威胁,如浏览黄色、暴力、反动等网站,以及由于

重要赢利模式之一。

## 8.3.1 校园网安全解决方案

校园网已成为各高等院校信息技术的基础设施，是学校可持续发展的重要保证。校园网总体上分为校园内网和校园外网。校园内网主要包括教学局域网、图书馆局域网、办公自动化局域网等。校园外网主要指学校提供对外服务的服务器群、与 Internet 的接入以及远程移动办公用户的接入等。校园网的服务器群构成了校园网的服务系统，主要包括 DNS、Web、FTP、MAIL、视频点播、教学平台等。外部网实现了校园网与 Internet 的基础接入，使院校教员和学生能使用电子邮件和浏览器等应用方式，在教学、科研和管理工作中利用国内和国际网进行信息交流和共享。校园网是校内外信息交流的窗口，也是高校教学、科研和行政管理不可缺少的重要基础设施。校园网结构开放，同时与教育网和 Internet 相连接。近年来，随着学生宿舍、教职工家属等接入校园网后，网络规模急剧增大，校园网用户组成复杂，用户水平参差不齐，其中不乏技术高超的黑客，这些因素使校园网的维护和管理变得十分困难。同时，校园网络的应用水平也在不断提高。规模的壮大和运用水平的提高就决定了校园网面临的隐患也相应加剧。由此可见，构筑网络安全防御体系是非常必要的。

### 1. 校园网安全隐患分析

当前校园网络存在的安全隐患和漏洞有如下几点。

(1) 校园网通过 CERNET 与 Internet 相连，在享受 Internet 方便快捷的同时，也面临着遭遇攻击的风险。即使有防火墙的保护，由于技术本身的局限或错误配置等原因，仍很难保证校园网不遭到黑客攻击。

(2) 校园网内部也存在很大的安全隐患，网络设备包括服务器、交换机、集线器、路由器、工作站、电源等分布在整个校园内，管理起来非常困难。由于内部用户对网络的结构和应用模式都比较了解，因此来自内部的安全威胁更大一些。现在，黑客攻击工具在网上泛滥成灾，大学生的好奇心理较强，决定了其利用这些工具进行攻击的可能性。部分学生可能出于各种目的在内部进行恶意操作，有意或无意地将它们损坏，经常会引发内部校园网安全危机，往往会造成校园网络全部或部分瘫痪。

(3) 目前网络服务器安装的操作系统有 Windows NT/Windows 2000、UNIX、Linux 等，这些系统安全风险级别不同，例如 Windows NT/Windows 2000 的普遍性和可操作性使得它也是最不安全的系统；UNIX 由于其技术的复杂性导致高级黑客对其进行攻击，这都对原有网络安全构成威胁。

(4) 随着校园内计算机应用的大范围普及，接入校园网节点日渐增多，而这些节点大部分都没有采取一定的防护措施，随时有可能造成病毒泛滥、信息丢失、数据损坏、网络被攻击、系统瘫痪等严重后果。例如，一些只对校园内部用户开放的服务，常常被设置后门。比较典型的例子，高校数字图书馆通常都限定只对内部 IP 开放，然而有的学生会在校内安置代理程序，供外部人员访问，造成学校信息的泄露。

(5) 内部用户对 Internet 的非法访问威胁，如浏览黄色、暴力、反动等网站，以及由于

重要赢利模式之一。

## 8.3.1 校园网安全解决方案

校园网已成为各高等院校信息技术的基础设施,是学校可持续发展的重要保证。校园网总体上分为校园内网和校园外网。校园内网主要包括教学局域网、图书馆局域网、办公自动化局域网等。校园外网主要指学校提供对外服务的服务器群、与 Internet 的接入以及远程移动办公用户的接入等。校园网的服务器群构成了校园网的服务系统,主要包括 DNS、Web、FTP、MAIL、视频点播、教学平台等。外部网实现了校园网与 Internet 的基础接入,使院校教员和学生能使用电子邮件和浏览器等应用方式,在教学、科研和管理工作中利用国内和国际网进行信息交流和共享。校园网是校内外信息交流的窗口,也是高校教学、科研和行政管理不可缺少的重要基础设施。校园网结构开放,同时与教育网和 Internet 相连接。近年来,随着学生宿舍、教职工家属等接入校园网后,网络规模急剧增大,校园网用户组成复杂,用户水平参差不齐,其中不乏技术高超的黑客,这些因素使校园网的维护和管理变得十分困难。同时,校园网络的应用水平也在不断提高。规模的壮大和运用水平的提高就决定了校园网面临的隐患也相应加剧。由此可见,构筑网络安全防御体系是非常必要的。

### 1. 校园网安全隐患分析

当前校园网络存在的安全隐患和漏洞有如下几点。

(1) 校园网通过 CERNET 与 Internet 相连,在享受 Internet 方便快捷的同时,也面临着遭遇攻击的风险。即使有防火墙的保护,由于技术本身的局限或错误配置等原因,仍很难保证校园网不遭到黑客攻击。

(2) 校园网内部也存在很大的安全隐患,网络设备包括服务器、交换机、集线器、路由器、工作站、电源等分布在整个校园内,管理起来非常困难。由于内部用户对网络的结构和应用模式都比较了解,因此来自内部的安全威胁更大一些。现在,黑客攻击工具在网上泛滥成灾,大学生的好奇心理较强,决定了其利用这些工具进行攻击的可能性。部分学生可能出于各种目的在内部进行恶意操作,有意或无意地将它们损坏,经常会引发内部校园网安全危机,往往会造成校园网络全部或部分瘫痪。

(3) 目前网络服务器安装的操作系统有 Windows NT/Windows 2000、UNIX、Linux 等,这些系统安全风险级别不同,例如 Windows NT/Windows 2000 的普遍性和可操作性使得它也是最不安全的系统;UNIX 由于其技术的复杂性导致高级黑客对其进行攻击,这都对原有网络安全构成威胁。

(4) 随着校园内计算机应用的大范围普及,接入校园网节点日渐增多,而这些节点大部分都没有采取一定的防护措施,随时有可能造成病毒泛滥、信息丢失、数据损坏、网络被攻击、系统瘫痪等严重后果。例如,一些只对校园内部用户开放的服务,常常被设置后门。比较典型的例子,高校数字图书馆通常都限定只对内部 IP 开放,然而有的学生会在校内安置代理程序,供外部人员访问,造成学校信息的泄露。

(5) 内部用户对 Internet 的非法访问威胁,如浏览黄色、暴力、反动等网站,以及由于

重要赢利模式之一。

## 8.3.1 校园网安全解决方案

校园网已成为各高等院校信息技术的基础设施，是学校可持续发展的重要保证。校园网总体上分为校园内网和校园外网。校园内网主要包括教学局域网、图书馆局域网、办公自动化局域网等。校园外网主要指学校提供对外服务的服务器群、与 Internet 的接入以及远程移动办公用户的接入等。校园网的服务器群构成了校园网的服务系统，主要包括 DNS、Web、FTP、MAIL、视频点播、教学平台等。外部网实现了校园网与 Internet 的基础接入，使院校教员和学生能使用电子邮件和浏览器等应用方式，在教学、科研和管理工作中利用国内和国际网进行信息交流和共享。校园网是校内外信息交流的窗口，也是高校教学、科研和行政管理不可缺少的重要基础设施。校园网结构开放，同时与教育网和 Internet 相连接。近年来，随着学生宿舍、教职工家属等接入校园网后，网络规模急剧增大，校园网用户组成复杂，用户水平参差不齐，其中不乏技术高超的黑客，这些因素使校园网的维护和管理变得十分困难。同时，校园网络的应用水平也在不断提高。规模的壮大和运用水平的提高就决定了校园网面临的隐患也相应加剧。由此可见，构筑网络安全防御体系是非常必要的。

### 1. 校园网安全隐患分析

当前校园网络存在的安全隐患和漏洞有如下几点。

(1) 校园网通过 CERNET 与 Internet 相连，在享受 Internet 方便快捷的同时，也面临着遭遇攻击的风险。即使有防火墙的保护，由于技术本身的局限或错误配置等原因，仍很难保证校园网不遭到黑客攻击。

(2) 校园网内部也存在很大的安全隐患，网络设备包括服务器、交换机、集线器、路由器、工作站、电源等分布在整个校园内，管理起来非常困难。由于内部用户对网络的结构和应用模式都比较了解，因此来自内部的安全威胁更大一些。现在，黑客攻击工具在网上泛滥成灾，大学生的好奇心理较强，决定了其利用这些工具进行攻击的可能性。部分学生可能出于各种目的在内部进行恶意操作，有意或无意地将它们损坏，经常会引发内部校园网安全危机，往往会造成校园网络全部或部分瘫痪。

(3) 目前网络服务器安装的操作系统有 Windows NT/Windows 2000、UNIX、Linux 等，这些系统安全风险级别不同，例如 Windows NT/Windows 2000 的普遍性和可操作性使得它也是最不安全的系统；UNIX 由于其技术的复杂性导致高级黑客对其进行攻击，这都对原有网络安全构成威胁。

(4) 随着校园内计算机应用的大范围普及，接入校园网节点日渐增多，而这些节点大部分都没有采取一定的防护措施，随时有可能造成病毒泛滥、信息丢失、数据损坏、网络被攻击、系统瘫痪等严重后果。例如，一些只对校园内部用户开放的服务，常常被设置后门。比较典型的例子，高校数字图书馆通常都限定只对内部 IP 开放，然而有的学生会在校内安置代理程序，供外部人员访问，造成学校信息的泄露。

(5) 内部用户对 Internet 的非法访问威胁，如浏览黄色、暴力、反动等网站，以及由于

重要赢利模式之一。

## 8.3.1 校园网安全解决方案

校园网已成为各高等院校信息技术的基础设施，是学校可持续发展的重要保证。校园网总体上分为校园内网和校园外网。校园内网主要包括教学局域网、图书馆局域网、办公自动化局域网等。校园外网主要指学校提供对外服务的服务器群、与 Internet 的接入以及远程移动办公用户的接入等。校园网的服务器群构成了校园网的服务系统，主要包括 DNS、Web、FTP、MAIL、视频点播、教学平台等。外部网实现了校园网与 Internet 的基础接入，使院校教员和学生能使用电子邮件和浏览器等应用方式，在教学、科研和管理工作中利用国内和国际网进行信息交流和共享。校园网是校内外信息交流的窗口，也是高校教学、科研和行政管理不可缺少的重要基础设施。校园网结构开放，同时与教育网和 Internet 相连接。近年来，随着学生宿舍、教职工家属等接入校园网后，网络规模急剧增大，校园网用户组成复杂，用户水平参差不齐，其中不乏技术高超的黑客，这些因素使校园网的维护和管理变得十分困难。同时，校园网络的应用水平也在不断提高。规模的壮大和运用水平的提高就决定了校园网面临的隐患也相应加剧。由此可见，构筑网络安全防御体系是非常必要的。

### 1. 校园网安全隐患分析

当前校园网络存在的安全隐患和漏洞有如下几点。

(1) 校园网通过 CERNET 与 Internet 相连，在享受 Internet 方便快捷的同时，也面临着遭遇攻击的风险。即使有防火墙的保护，由于技术本身的局限或错误配置等原因，仍很难保证校园网不遭到黑客攻击。

(2) 校园网内部也存在很大的安全隐患，网络设备包括服务器、交换机、集线器、路由器、工作站、电源等分布在整个校园内，管理起来非常困难。由于内部用户对网络的结构和应用模式都比较了解，因此来自内部的安全威胁更大一些。现在，黑客攻击工具在网上泛滥成灾，大学生的好奇心理较强，决定了其利用这些工具进行攻击的可能性。部分学生可能出于各种目的在内部进行恶意操作，有意或无意地将它们损坏，经常会引发内部校园网安全危机，往往会造成校园网络全部或部分瘫痪。

(3) 目前网络服务器安装的操作系统有 Windows NT/Windows 2000、UNIX、Linux 等，这些系统安全风险级别不同，例如 Windows NT/Windows 2000 的普遍性和可操作性使得它也是最不安全的系统；UNIX 由于其技术的复杂性导致高级黑客对其进行攻击，这都对原有网络安全构成威胁。

(4) 随着校园内计算机应用的大范围普及，接入校园网节点日渐增多，而这些节点大部分都没有采取一定的防护措施，随时有可能造成病毒泛滥、信息丢失、数据损坏、网络被攻击、系统瘫痪等严重后果。例如，一些只对校园内部用户开放的服务，常常被设置后门。比较典型的例子，高校数字图书馆通常都限定只对内部 IP 开放，然而有的学生会在校内安置代理程序，供外部人员访问，造成学校信息的泄露。

(5) 内部用户对 Internet 的非法访问威胁，如浏览黄色、暴力、反动等网站，以及由于

重要赢利模式之一。

## 8.3.1 校园网安全解决方案

校园网已成为各高等院校信息技术的基础设施，是学校可持续发展的重要保证。校园网总体上分为校园内网和校园外网。校园内网主要包括教学局域网、图书馆局域网、办公自动化局域网等。校园外网主要指学校提供对外服务的服务器群、与 Internet 的接入以及远程移动办公用户的接入等。校园网的服务器群构成了校园网的服务系统，主要包括 DNS、Web、FTP、MAIL、视频点播、教学平台等。外部网实现了校园网与 Internet 的基础接入，使院校教员和学生能使用电子邮件和浏览器等应用方式，在教学、科研和管理工作中利用国内和国际网进行信息交流和共享。校园网是校内外信息交流的窗口，也是高校教学、科研和行政管理不可缺少的重要基础设施。校园网结构开放，同时与教育网和 Internet 相连接。近年来，随着学生宿舍、教职工家属等接入校园网后，网络规模急剧增大，校园网用户组成复杂，用户水平参差不齐，其中不乏技术高超的黑客，这些因素使校园网的维护和管理变得十分困难。同时，校园网络的应用水平也在不断提高。规模的壮大和运用水平的提高就决定了校园网面临的隐患也相应加剧。由此可见，构筑网络安全防御体系是非常必要的。

### 1. 校园网安全隐患分析

当前校园网络存在的安全隐患和漏洞有如下几点。

(1) 校园网通过 CERNET 与 Internet 相连，在享受 Internet 方便快捷的同时，也面临着遭遇攻击的风险。即使有防火墙的保护，由于技术本身的局限或错误配置等原因，仍很难保证校园网不遭到黑客攻击。

(2) 校园网内部也存在很大的安全隐患，网络设备包括服务器、交换机、集线器、路由器、工作站、电源等分布在整个校园内，管理起来非常困难。由于内部用户对网络的结构和应用模式都比较了解，因此来自内部的安全威胁更大一些。现在，黑客攻击工具在网上泛滥成灾，大学生的好奇心理较强，决定了其利用这些工具进行攻击的可能性。部分学生可能出于各种目的在内部进行恶意操作，有意或无意地将它们损坏，经常会引发内部校园网安全危机，往往会造成校园网络全部或部分瘫痪。

(3) 目前网络服务器安装的操作系统有 Windows NT/Windows 2000、UNIX、Linux 等，这些系统安全风险级别不同，例如 Windows NT/Windows 2000 的普遍性和可操作性使得它也是最不安全的系统；UNIX 由于其技术的复杂性导致高级黑客对其进行攻击，这都对原有网络安全构成威胁。

(4) 随着校园内计算机应用的大范围普及，接入校园网节点日渐增多，而这些节点大部分都没有采取一定的防护措施，随时有可能造成病毒泛滥、信息丢失、数据损坏、网络被攻击、系统瘫痪等严重后果。例如，一些只对校园内部用户开放的服务，常常被设置后门。比较典型的例子，高校数字图书馆通常都限定只对内部 IP 开放，然而有的学生会在校内安置代理程序，供外部人员访问，造成学校信息的泄露。

(5) 内部用户对 Internet 的非法访问威胁，如浏览黄色、暴力、反动等网站，以及由于

重要赢利模式之一。

## 8.3.1 校园网安全解决方案

校园网已成为各高等院校信息技术的基础设施，是学校可持续发展的重要保证。校园网总体上分为校园内网和校园外网。校园内网主要包括教学局域网、图书馆局域网、办公自动化局域网等。校园外网主要指学校提供对外服务的服务器群、与 Internet 的接入以及远程移动办公用户的接入等。校园网的服务器群构成了校园网的服务系统，主要包括 DNS、Web、FTP、MAIL、视频点播、教学平台等。外部网实现了校园网与 Internet 的基础接入，使院校教员和学生能使用电子邮件和浏览器等应用方式，在教学、科研和管理工作中利用国内和国际网进行信息交流和共享。校园网是校内外信息交流的窗口，也是高校教学、科研和行政管理不可缺少的重要基础设施。校园网结构开放，同时与教育网和 Internet 相连接。近年来，随着学生宿舍、教职工家属等接入校园网后，网络规模急剧增大，校园网用户组成复杂，用户水平参差不齐，其中不乏技术高超的黑客，这些因素使校园网的维护和管理变得十分困难。同时，校园网络的应用水平也在不断提高。规模的壮大和运用水平的提高就决定了校园网面临的隐患也相应加剧。由此可见，构筑网络安全防御体系是非常必要的。

### 1. 校园网安全隐患分析

当前校园网络存在的安全隐患和漏洞有如下几点。

(1) 校园网通过 CERNET 与 Internet 相连，在享受 Internet 方便快捷的同时，也面临着遭遇攻击的风险。即使有防火墙的保护，由于技术本身的局限或错误配置等原因，仍很难保证校园网不遭到黑客攻击。

(2) 校园网内部也存在很大的安全隐患，网络设备包括服务器、交换机、集线器、路由器、工作站、电源等分布在整个校园内，管理起来非常困难。由于内部用户对网络的结构和应用模式都比较了解，因此来自内部的安全威胁更大一些。现在，黑客攻击工具在网上泛滥成灾，大学生的好奇心理较强，决定了其利用这些工具进行攻击的可能性。部分学生可能出于各种目的在内部进行恶意操作，有意或无意地将它们损坏，经常会引发内部校园网安全危机，往往会造成校园网络全部或部分瘫痪。

(3) 目前网络服务器安装的操作系统有 Windows NT/Windows 2000、UNIX、Linux 等，这些系统安全风险级别不同，例如 Windows NT/Windows 2000 的普遍性和可操作性使得它也是最不安全的系统；UNIX 由于其技术的复杂性导致高级黑客对其进行攻击，这都对原有网络安全构成威胁。

(4) 随着校园内计算机应用的大范围普及，接入校园网节点日渐增多，而这些节点大部分都没有采取一定的防护措施，随时有可能造成病毒泛滥、信息丢失、数据损坏、网络被攻击、系统瘫痪等严重后果。例如，一些只对校园内部用户开放的服务，常常被设置后门。比较典型的例子，高校数字图书馆通常都限定只对内部 IP 开放，然而有的学生会在校内安置代理程序，供外部人员访问，造成学校信息的泄露。

(5) 内部用户对 Internet 的非法访问威胁，如浏览黄色、暴力、反动等网站，以及由于

重要赢利模式之一。

## 8.3.1 校园网安全解决方案

校园网已成为各高等院校信息技术的基础设施，是学校可持续发展的重要保证。校园网总体上分为校园内网和校园外网。校园内网主要包括教学局域网、图书馆局域网、办公自动化局域网等。校园外网主要指学校提供对外服务的服务器群、与 Internet 的接入以及远程移动办公用户的接入等。校园网的服务器群构成了校园网的服务系统，主要包括 DNS、Web、FTP、MAIL、视频点播、教学平台等。外部网实现了校园网与 Internet 的基础接入，使院校教员和学生能使用电子邮件和浏览器等应用方式，在教学、科研和管理工作中利用国内和国际网进行信息交流和共享。校园网是校内外信息交流的窗口，也是高校教学、科研和行政管理不可缺少的重要基础设施。校园网结构开放，同时与教育网和 Internet 相连接。近年来，随着学生宿舍、教职工家属等接入校园网后，网络规模急剧增大，校园网用户组成复杂，用户水平参差不齐，其中不乏技术高超的黑客，这些因素使校园网的维护和管理变得十分困难。同时，校园网络的应用水平也在不断提高。规模的壮大和运用水平的提高就决定了校园网面临的隐患也相应加剧。由此可见，构筑网络安全防御体系是非常必要的。

### 1. 校园网安全隐患分析

当前校园网络存在的安全隐患和漏洞有如下几点。

(1) 校园网通过 CERNET 与 Internet 相连，在享受 Internet 方便快捷的同时，也面临着遭遇攻击的风险。即使有防火墙的保护，由于技术本身的局限或错误配置等原因，仍很难保证校园网不遭到黑客攻击。

(2) 校园网内部也存在很大的安全隐患，网络设备包括服务器、交换机、集线器、路由器、工作站、电源等分布在整个校园内，管理起来非常困难。由于内部用户对网络的结构和应用模式都比较了解，因此来自内部的安全威胁更大一些。现在，黑客攻击工具在网上泛滥成灾，大学生的好奇心理较强，决定了其利用这些工具进行攻击的可能性。部分学生可能出于各种目的在内部进行恶意操作，有意或无意地将它们损坏，经常会引发内部校园网安全危机，往往会造成校园网络全部或部分瘫痪。

(3) 目前网络服务器安装的操作系统有 Windows NT/Windows 2000、UNIX、Linux 等，这些系统安全风险级别不同，例如 Windows NT/Windows 2000 的普遍性和可操作性使得它也是最不安全的系统；UNIX 由于其技术的复杂性导致高级黑客对其进行攻击，这都对原有网络安全构成威胁。

(4) 随着校园内计算机应用的大范围普及，接入校园网节点日渐增多，而这些节点大部分都没有采取一定的防护措施，随时有可能造成病毒泛滥、信息丢失、数据损坏、网络被攻击、系统瘫痪等严重后果。例如，一些只对校园内部用户开放的服务，常常被设置后门。比较典型的例子，高校数字图书馆通常都限定只对内部 IP 开放，然而有的学生会在校内安置代理程序，供外部人员访问，造成学校信息的泄露。

(5) 内部用户对 Internet 的非法访问威胁，如浏览黄色、暴力、反动等网站，以及由于

重要赢利模式之一。

## 8.3.1 校园网安全解决方案

校园网已成为各高等院校信息技术的基础设施，是学校可持续发展的重要保证。校园网总体上分为校园内网和校园外网。校园内网主要包括教学局域网、图书馆局域网、办公自动化局域网等。校园外网主要指学校提供对外服务的服务器群、与 Internet 的接入以及远程移动办公用户的接入等。校园网的服务器群构成了校园网的服务系统，主要包括 DNS、Web、FTP、MAIL、视频点播、教学平台等。外部网实现了校园网与 Internet 的基础接入，使院校教员和学生能使用电子邮件和浏览器等应用方式，在教学、科研和管理工作中利用国内和国际网进行信息交流和共享。校园网是校内外信息交流的窗口，也是高校教学、科研和行政管理不可缺少的重要基础设施。校园网结构开放，同时与教育网和 Internet 相连接。近年来，随着学生宿舍、教职工家属等接入校园网后，网络规模急剧增大，校园网用户组成复杂，用户水平参差不齐，其中不乏技术高超的黑客，这些因素使校园网的维护和管理变得十分困难。同时，校园网络的应用水平也在不断提高。规模的壮大和运用水平的提高就决定了校园网面临的隐患也相应加剧。由此可见，构筑网络安全防御体系是非常必要的。

### 1. 校园网安全隐患分析

当前校园网络存在的安全隐患和漏洞有如下几点。

(1) 校园网通过 CERNET 与 Internet 相连，在享受 Internet 方便快捷的同时，也面临着遭遇攻击的风险。即使有防火墙的保护，由于技术本身的局限或错误配置等原因，仍很难保证校园网不遭到黑客攻击。

(2) 校园网内部也存在很大的安全隐患，网络设备包括服务器、交换机、集线器、路由器、工作站、电源等分布在整个校园内，管理起来非常困难。由于内部用户对网络的结构和应用模式都比较了解，因此来自内部的安全威胁更大一些。现在，黑客攻击工具在网上泛滥成灾，大学生的好奇心理较强，决定了其利用这些工具进行攻击的可能性。部分学生可能出于各种目的在内部进行恶意操作，有意或无意地将它们损坏，经常会引发内部校园网安全危机，往往会造成校园网络全部或部分瘫痪。

(3) 目前网络服务器安装的操作系统有 Windows NT/Windows 2000、UNIX、Linux 等，这些系统安全风险级别不同，例如 Windows NT/Windows 2000 的普遍性和可操作性使得它也是最不安全的系统；UNIX 由于其技术的复杂性导致高级黑客对其进行攻击，这都对原有网络安全构成威胁。

(4) 随着校园内计算机应用的大范围普及，接入校园网节点日渐增多，而这些节点大部分都没有采取一定的防护措施，随时有可能造成病毒泛滥、信息丢失、数据损坏、网络被攻击、系统瘫痪等严重后果。例如，一些只对校园内部用户开放的服务，常常被设置后门。比较典型的例子，高校数字图书馆通常都限定只对内部 IP 开放，然而有的学生会在校内安置代理程序，供外部人员访问，造成学校信息的泄露。

(5) 内部用户对 Internet 的非法访问威胁，如浏览黄色、暴力、反动等网站，以及由于

重要赢利模式之一。

## 8.3.1 校园网安全解决方案

校园网已成为各高等院校信息技术的基础设施，是学校可持续发展的重要保证。校园网总体上分为校园内网和校园外网。校园内网主要包括教学局域网、图书馆局域网、办公自动化局域网等。校园外网主要指学校提供对外服务的服务器群、与 Internet 的接入以及远程移动办公用户的接入等。校园网的服务器群构成了校园网的服务系统，主要包括 DNS、Web、FTP、MAIL、视频点播、教学平台等。外部网实现了校园网与 Internet 的基础接入，使院校教员和学生能使用电子邮件和浏览器等应用方式，在教学、科研和管理工作中利用国内和国际网进行信息交流和共享。校园网是校内外信息交流的窗口，也是高校教学、科研和行政管理不可缺少的重要基础设施。校园网结构开放，同时与教育网和 Internet 相连接。近年来，随着学生宿舍、教职工家属等接入校园网后，网络规模急剧增大，校园网用户组成复杂，用户水平参差不齐，其中不乏技术高超的黑客，这些因素使校园网的维护和管理变得十分困难。同时，校园网络的应用水平也在不断提高。规模的壮大和运用水平的提高就决定了校园网面临的隐患也相应加剧。由此可见，构筑网络安全防御体系是非常必要的。

### 1. 校园网安全隐患分析

当前校园网络存在的安全隐患和漏洞有如下几点。

(1) 校园网通过 CERNET 与 Internet 相连，在享受 Internet 方便快捷的同时，也面临着遭遇攻击的风险。即使有防火墙的保护，由于技术本身的局限或错误配置等原因，仍很难保证校园网不遭到黑客攻击。

(2) 校园网内部也存在很大的安全隐患，网络设备包括服务器、交换机、集线器、路由器、工作站、电源等分布在整个校园内，管理起来非常困难。由于内部用户对网络的结构和应用模式都比较了解，因此来自内部的安全威胁更大一些。现在，黑客攻击工具在网上泛滥成灾，大学生的好奇心理较强，决定了其利用这些工具进行攻击的可能性。部分学生可能出于各种目的在内部进行恶意操作，有意或无意地将它们损坏，经常会引发内部校园网安全危机，往往会造成校园网络全部或部分瘫痪。

(3) 目前网络服务器安装的操作系统有 Windows NT/Windows 2000、UNIX、Linux 等，这些系统安全风险级别不同，例如 Windows NT/Windows 2000 的普遍性和可操作性使得它也是最不安全的系统；UNIX 由于其技术的复杂性导致高级黑客对其进行攻击，这都对原有网络安全构成威胁。

(4) 随着校园内计算机应用的大范围普及，接入校园网节点日渐增多，而这些节点大部分都没有采取一定的防护措施，随时有可能造成病毒泛滥、信息丢失、数据损坏、网络被攻击、系统瘫痪等严重后果。例如，一些只对校园内部用户开放的服务，常常被设置后门。比较典型的例子，高校数字图书馆通常都限定只对内部 IP 开放，然而有的学生会在校内安置代理程序，供外部人员访问，造成学校信息的泄露。

(5) 内部用户对 Internet 的非法访问威胁，如浏览黄色、暴力、反动等网站，以及由于

下载文件可能将木马、蠕虫、病毒等程序带入校园内网。内外网恶意用户可能利用一些工具对网络及服务器发起 DoS/DDoS 攻击,导致网络及服务不可用。校园网内的学生群体是主要的 OICQ 用户,目前针对 OICQ 的黑客程序随处可见。

(6) 可能会因为校园网内管理人员以及全体师生的安全意识不强、管理制度不健全,带来校园网的威胁。

根据校园网的结构特点及面临的安全隐患,确定了以下几个必须考虑的安全防护要点:网络安全隔离、网络监控措施、网络安全漏洞、网络病毒的防范。

### 2. 防火墙部署

在 Internet 与校园网内网之间部署一台防火墙,成为内外网之间一道牢固的安全屏障。其中 WWW、MAIL、FTP、DNS 对外服务器连接在防火墙的 DMZ 区,与内、外网间进行隔离,内网口连接校园网内网交换机,外网口通过路由器与 Internet 连接。那么,通过 Internet 进来的公众用户只能访问到对外公开的一些服务(如 WWW、MAIL、FTP、DNS 等),既保护内网资源不被外部非授权用户非法访问或破坏,也可以阻止内部用户对外部不良资源的滥用,还能够对发生在网络中的安全事件进行跟踪和审计。在防火墙设置上按照以下原则配置来提高网络安全性。

(1) 根据校园网安全策略和安全目标,规划设置正确的安全过滤规则,规则审核 IP 数据包的内容包括协议、端口、源地址、目的地址、流向等项目,严格禁止来自公网对校园内部网不必要的、非法的访问。总体上遵从"不被允许的服务就是被禁止"的原则。

(2) 将防火墙配置成过滤掉以内部网络地址进入路由器的 IP 包,这样可以防范源地址假冒和源路由类型的攻击;过滤掉以非法 IP 地址离开内部网络的 IP 包,防止内部网络发起的对外攻击。

(3) 在防火墙上建立内网计算机的 IP 地址和 MAC 地址的对应表,防止 IP 地址被盗用。

(4) 定期查看防火墙访问日志,及时发现攻击行为和不良上网记录。

(5) 允许通过配置网卡对防火墙设置,提高防火墙管理安全性。

### 3. 入侵检测系统部署

入侵检测能力是衡量一个防御体系是否完整有效的重要因素,强大完整的入侵检测体系可以弥补防火墙相对静态防御的不足。根据学校网络的特点,对来自外部网和校园网内部的各种行为进行实时检测,及时发现各种可能的攻击企图,并采取相应的措施。具体来讲,就是将入侵检测引擎接入核心交换机上。入侵检测系统集入侵检测、网络管理和网络监视功能于一身,能实时捕获内外网之间传输的所有数据,利用内置的攻击特征库,使用模式匹配和智能分析的方法,检测网络上发生的入侵行为和异常现象,并在数据库中记录有关事件,作为网络管理员事后分析的依据。如果情况严重,入侵检测系统可以发出实时报警,使得学校管理员能够及时采取应对措施。

### 4. 漏洞扫描系统

采用目前最先进的漏洞扫描系统定期对工作站、服务器、交换机等进行安全检查，并根据检查结果向系统管理员提供详细可靠的安全性分析报告，为提高网络安全整体水平产生重要依据。

### 5. 病毒防范部署

在该网络防病毒方案中，最终要达到一个目的就是要在整个局域网内杜绝病毒的感染、传播和发作。为了实现这一点，应该在整个网络内可能感染和传播病毒的地方采取相应的防病毒手段。同时为了有效、快捷地实施和管理整个网络的防病毒体系，应能实现远程安装、智能升级、远程报警、集中管理、分步查杀等多种功能。

（1）在学校网络中心安装配置一个杀毒软件网络版的系统中心，负责管理全校主机网点的计算机，同时在各客户计算机上分别安装杀毒软件网络版的客户端。

（2）安装完杀毒软件网络版后，在管理员控制台对网络中所有客户端进行定时查杀毒的设置，保证所有客户端即使在没有联网的时候也能够定时进行对本机的查杀。

（3）网络中心负责整个校园网的升级工作。为了安全和管理的方便起见，由网络中心的系统中心定期地、自动地到杀毒软件公司的网站上获取最新的升级文件(包括病毒定义码、扫描引擎、程序文件等)，然后自动将最新的升级文件分发到其他用户的客户端与服务器端，并自动对杀毒软件网络版进行更新。采取这种升级方式，一方面确保校园网内的杀毒软件的更新保持同步，使整个校园网都具有最强的防病毒能力。另一方面由于整个网络的升级、更新都是有程序来自动、智能完成，就可以避免由于人为因素造成网络中因为没有及时升级而失去最强的防病毒能力。

### 6. 安全管理

常言说："三分技术，七分管理"，安全管理是保证网络安全的基础，安全技术是配合安全管理的辅助措施。要建立一套校园网络安全管理模式，制定详细的安全管理制度，如机房管理制度、病毒防范制度等，并采取切实有效的措施保证制度的执行。

校园网整体安全解决方案如图 8-17 所示。

## 8.3.2 大型企业网络安全解决方案

综合考虑大型企业系统的现状、安全建设目标和上述的方案设计原则，大型企业系统的安全解决方案，由 5 部分组成：远程接入安全解决方案、边界安全解决方案、内网安全解决方案、数据中心安全解决方案、全局安全管理解决方案。

这五部分的安全解决方案衔接在一起构成了一个覆盖大型企业系统网络"端到端"信息流程的"全网安全解决方案"，是一个内容全面，可分步实施，可持续演进的解决方案集。

### 1. 远程接入安全解决方案

对拥有异地分支的大型企业系统来说，为提高沟通效率和资源利用效率，建立分支

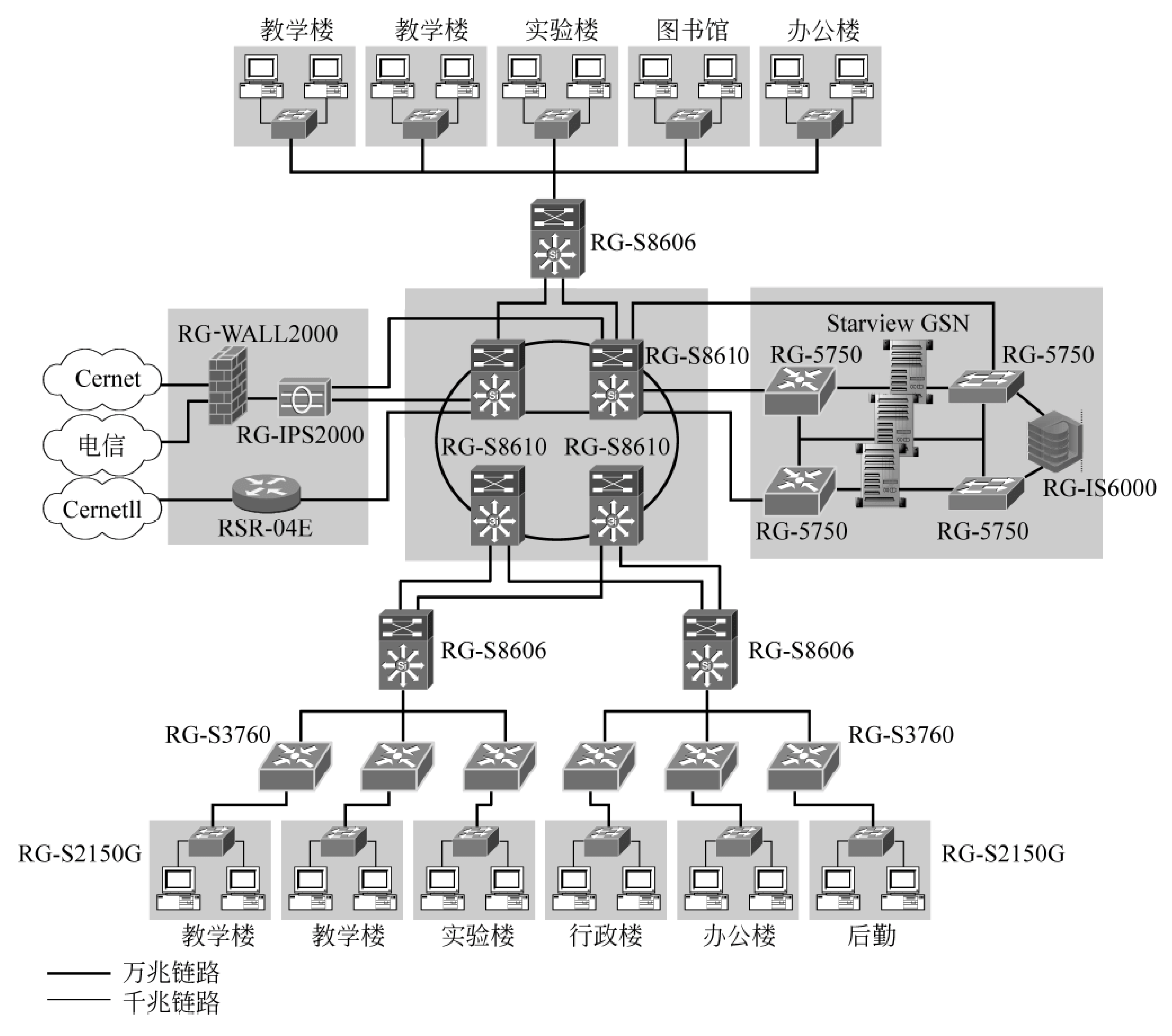



**图 8-17　高等学校网络安全解决方案**

与总部之间的具有保密性的网络连接是十分必要的。此外，大型企业系统的工作人员出差时也需要访问系统内部的一些信息资源，这时同样需要建立保密的网络连接。虚拟专用网技术以其灵活、安全、经济、易扩展的特点，满足这部分需求。

1）IPSec VPN 解决方案

IPSec 是业界标准的网络安全协议，可以为 IP 网络通信提供加密服务，保护 TCP/IP 通信免遭窃听和篡改，从而有效抵御网络攻击。IPSec VPN 解决方案，由 VPN 接入网关和 VPN 管理子系统两个部分组成。

VPN 接入网关是整个 VPN 系统的核心部分。它支持多种 VPN 业务，如 L2TP VPN、IPSec VPN、GRE VPN、MPLS VPN 等，它可以针对客户需求通过拨号、租用线、VLAN 或隧道等方式接入远端用户，构建 Internet、Intranet、Extranet 等多种形式的 VPN。

(1) IPSec VPN 解决方案的特点。

① 组网灵活：从用户业务需求、可靠性要求和投资规模等方面综合考虑，设计了多种分支上联总部的解决方案，包括单链路单网关、单链路双网关和双链路双网关。

② 管理简单：采用专门的管理系统，其图形化的管理界面使维护更简单。支持自动

发现和构建 VPN 拓扑，直观查看 VPN 通道状态、通道流量情况、VPN 设备的运行情况等。

③ 集中配置：机构分布广、设备多、配置重复，往往给设备管理带来繁重的工作量，系统采用分支设备主动、网管被动的方式对分支的设备进行管理，网络连接由分支设备主动发起，公私网地址转换、动态 IP 地址、批量设备配置等难题迎刃而解。

（2）IPSec VPN 解决方案的典型组网。

在实际的组网中，可以根据大型企业系统的情况，采用灵活多样的组网方式，用最低的代价满足大型企业系统 VPN 接入需求。

① 单链路单网关。

该组网方案采用单链路单网关方式，在总部局域网数据中心部署 VPN 管理组件，实现对 VPN 网关的部署管理和监控，在总部局域网内部或 Internet 边界部署管理系统，实现对分支机构 VPN 网关设备的自动配置和策略部署。

该方案主要面向对网络链路可靠性要求不高的情况，可采用 IPSec VPN、IPSec over GRE VPN、GRE over IPSec VPN、L2TP over IPSec VPN 等方式实现接入。

② 单链路双网关。

该组网方案采用单链路双网关方式，对 VPN 网关进行了双机备份，适用于对可靠性要求较高的情况。可采用 L2TP、VRRP、OSPF 方式实现网关间的备份。

③ 双链路双网关。

该组网方案在 VPN 网关备份的基础上，对于接入分支节点的链路也进行了备份。不同链路分别接入到不同的 ISP（电信、网通），主链路采用光纤接入，备份链路采用 ADSL 进行热备。为了增强 VPN 网关的稳定性，在 VPN 网关节点部署双 VPN 网关，利用该 VPN 双网关可以有效地提高系统的可靠性。该方案主要面向特别重要、对可靠性要求非常高的分支机构。

2）SSL VPN 解决方案

IPSec VPN 帮助大型企业系统解决了分支安全接入总部的问题。但是它无法解决移动办公用户（出差人员）远程接入的问题，SSL VPN 解决方案正好满足了这部分需求，而且 SSL VPN 具有细粒度控制、免客户端软件安装等其他特点。

整个解决方案基于 B/S 架构，客户端不需要安装特殊软件，通过 Web 浏览器直接访问 SSL VPN 网关，输入用户名和密码即可安全地访问企业内部网络资源。

SSL VPN 解决方案特点如下。

（1）接入灵活：采用 B/S 架构，直接使用浏览器完成 VPN 接入。当员工需要进行远程接入时，其移动终端不需要特别配置，降低了维护成本和使用难度。

（2）细化控制：能够根据用户个人身份和主机安全状态授予其不同的访问权限。在面向合作伙伴时，也可以根据情况，灵活地授予合作伙伴不同的访问权限。

（3）个性化界面：可以定制个性化的用户界面。系统管理员能够调整访问界面，以符合大型企业系统内部网络的风格，包括更换 LOGO 和定制布局等。

### 2. 边界安全解决方案

随着大型企业系统网络上IT应用的不断增加以及网络中设备的增加，网络边界安全成为最重要的安全问题之一，需要组合型的安全解决方案。

1）边界安全解决方案概述

对大型企业系统边界进行安全防护，首先必须明确哪些网络边界需要防护，这可以通过安全分区来确定。定义安全分区的原则就是首先根据业务和信息敏感度定义安全资产，其次对安全资产定义安全策略和安全级别，对于安全策略和级别相同的安全资产，就可以认为属于同一安全区域。根据以上原则，提出大型企业系统的安全分区模型，主要包括内网办公区、数据中心区、外联数据区、互联网连接区、对外连接区、网络管理区、广域网连接区等。

参照以上的分区，考虑到当前网络上的主要威胁，以防火墙、入侵检测防御系统(IDS、IPS)为支撑的边界安全解决方案。

(1) 防火墙：最主流也是最重要的安全产品，是边界安全解决方案的核心。它可以对整个网络进行区域分割，提供基于IP地址和TCP/IP服务端口等的访问控制。对常见的网络攻击，如拒绝服务攻击、端口扫描、IP欺骗、IP盗用等进行有效防护。并提供NAT地址转换、流量限制、用户认证、IP与MAC绑定等安全增强措施。由于防火墙部署在网关位置，也可以在防火墙中集成防病毒模块和网络安全监控模块。

(2) 入侵防御：传统的安全解决方案中，防火墙和入侵检测系统(intrusion detection system，IDS)已经被普遍接受，但仅仅有防火墙和IDS还不足以完全保护网络不受攻击。防火墙作为一个网络层的安全设备，不能充分地分析应用层协议数据中的攻击信号，而IDS也不能阻挡检测到的攻击。因此，即使在网络中已部署了防火墙、IDS等基础网络安全产品，IT部门仍然发现网络的带宽利用率居高不下，应用系统的响应速度越来越慢。产生这个问题的原因并不是当初网络设计不周，而是近年来蠕虫、P2P、木马等安全威胁日益滋长并演变到应用层面的结果，必须有相应的技术手段和解决方案来解决针对应用层的安全威胁。以入侵防御系统(intrusion prevention system，IPS)为代表的应用层安全设备，作为防火墙的重要补充，很好地解决了应用层防御的问题，并且变革了管理员构建网络防御的方式。通过在线部署，IPS可以检测并直接阻断恶意流量。

2）边界安全解决方案的典型部署

在大型企业系统互联网出口部署防火墙(集成防病毒和网络安全监控模块)和IPS设备，同时通过防火墙和IPS将企业内部网、DMZ、数据中心、互联网等安全区域分隔开，并通过制定相应的安全规则，以实现各区域不同级别、不同层次的安全防护。

3）边界安全解决方案特点

(1) 全面防护：在安全区域规划基础上，在网络边界部署防火墙、IPS等安全设备，能够实现网络2至7层的威胁抵御，形成动态、立体的全面安全防护。

(2) 深层防护：通过防火墙和IPS的部署，可以形成有效的深层次安全防护，如对蠕虫的传播和攻击进行防御、对P2P应用禁止和限流、抵抗DoS/DDoS的攻击等。

### 3. 内网安全解决方案

统计表明，在所有的安全事件中，有超过70%是发生在内网上的，并且随着网络的庞大化和复杂化，这一比例仍有增长的趋势。因此内网安全一直是网络安全建设关注的重点，但是由于内网以纯二层交换环境为主、节点数量多、分布复杂、终端用户安全应用水平参差不齐等原因，一直以来也都是安全建设的难点。

1）内网安全考虑的因素

一般说来，内网安全应该考虑以下问题。

（1）终端安全策略部署。

终端安全是内网安全的核心问题，终端安全策略的部署也就是内网安全的最主要部分。但是受限于终端用户安全应用水平，如何确保网络中的终端安全状态符合企业安全策略，却是每一个网络管理员不得不面对的挑战。管理员查找、隔离、修复不符合安全策略的终端，是一项费时费力的工作，往往造成企业安全策略与终端安全实施之间存在巨大的差距。

（2）内网访问控制部署。

传统上，在内网是通过划分VLAN，配合ACL进行访问控制，这虽然可以在一定程度上实现内网访问控制，却难以做到比较精细的安全控制，同时也可能会影响到VLAN间用户的访问，从而影响网络的使用效率。对于部分交换机，ACL数量的增加会导致严重的性能下降。如何在内网实现更精细更高效率的访问控制是内网安全建设必须要解决的问题。

（3）网络自身安全保障。

目前在内网安全事件中，出现从攻击主机转为攻击网络资源的趋势，而传统的以太网交换机的工作原理和开放特征决定其难以对此类攻击进行有效防控。

2）内网安全解决方案概述

内网安全解决方案考虑到内网安全的方方面面，针对上述内网安全的主要问题都提出了有针对性的技术，这些技术相互关联、相互配合，形成完善的内网安全解决方案。

（1）端点准入防御解决终端合规性问题。

为了解决现有安全防御体系中存在的不足，建立端点准入防御，旨在整合孤立的单点防御系统，加强对用户的集中管理，统一实施大型企业系统的安全策略，提高网络终端的主动抵抗能力。

端点准入防御将防病毒、补丁修复等终端安全措施与网络接入控制、访问权限控制等网络安全措施整合为一个联动的安全体系，通过对网络接入终端的检查、隔离、修复、管理和监控，使整个网络变被动防御为主动防御、变单点防御为全面防御、变分散管理为集中策略管理，提升了网络对病毒、蠕虫等新兴安全威胁的整体防御能力。

端点准入防御通过安全客户端、安全策略服务器、接入设备以及病毒库服务器、补丁服务器的相互配合，可以将不符合安全要求的终端限制在“隔离区”内，防止“危险”终端对网络安全的损害，避免“易感”终端受病毒、蠕虫的攻击。其主要功能包括如下几个。

① 检查用户终端的安全状态，配合不同方式的身份验证技术，可以确保接入终端的

合法与安全。

② 隔离违规终端。不符合企业安全策略的终端，将被限制访问权限，只能访问“隔离区”内的病毒库/补丁服务器等用于系统修复的网络资源。

③ 与第三方服务器中的补丁服务器、病毒服务器等形成联动，强制终端安装系统补丁、升级防病毒软件，直到满足安全策略要求。

④ 端点准入防御提供了集接入策略、安全策略、服务策略、安全事件监控于一体的用户管理平台，可以帮助网络管理员定制基于用户身份的、个性化的网络安全策略。同时端点准入防御可以通过安全策略服务器与安全客户端的配合，强制实施终端安全配置(如是否实时检查邮件、注册表、是否限制代理、是否限制双网卡等)，监控用户终端的安全事件(如查杀病毒、修改安全设置等)。

此外，端口隔离也是内网访问控制的一个有效手段。端口隔离是指交换机可以由硬件实现相同 VLAN 中的两个端口互相隔离。隔离后这两个端口在本设备内不能实现二、三层互通。当相同 VLAN 中的主机之间没有互访要求时，可以设置各自连接的端口为隔离端口。这样可以更好地保证相同安全区域内主机之间的安全。即使非法用户利用后门控制了其中一台主机，也无法利用该主机作为跳板攻击该安全区域内的其他主机。并且可以有效地隔离蠕虫病毒的传播，减小受感染主机可能造成的危害。

(2) 交换机安全特性实现网络自身安全保障。

以太网在设计时没有考虑安全性的要求，这造成了以太网自身存在很多的安全隐患，正是这种原因，目前出现了从攻击主机向攻击网络资源转变的趋势。

基于在以太网安全领域积累的大量经验，在交换机中提供了大量的安全特性，可以充分保障以太网的安全。这些安全特性同时也是内网安全解决方案中很多功能实现的基础，例如在端点准入防御解决方案中就使用到了接入交换机的 Port Security 特性。这些安全特性包括如下。

- 接入控制技术——Port Security；
- 接入安全技术——防 IP 伪装；
- 防中间人攻击——STP Root / BPDU 保护；
- 防 ARP 欺骗；
- 防 STP 攻击；
- DHCP Server 保护；
- 路由协议攻击防护能力。

3) 内网安全解决方案特点

(1) 内网统一安全策略实施：本方案不仅仅可以在网络设备上实施统一的安全策略，还可以实施终端安全策略，以达到整个内网安全策略统一实施的目的。

(2) 可扩展的安全解决方案：本方案是一个可扩展的安全解决方案，对现有网络设备和组网方式改造较小。在现有大型企业系统网络中，只需对网络设备进行简单升级，即可实现。

### 4. 数据中心安全解决方案

数据集中是管理集约化、精细化的必然要求，也是大型企业系统优化业务流程、管理流程的必要手段。作为网络中数据交换最频繁、资源最密集的地方，大型企业系统的数据中心出现任何安全防护上的疏漏必将导致不可估量的损失，因此数据中心安全解决方案十分重要。

1）数据中心面临的安全威胁分析

随着 Internet 应用日益深化，数据中心运行环境正从传统的客户端/服务器(C/S)架构向浏览器/服务器(B/S)架构转型，这意味着“瘦客户端，胖数据中心”成为必然的发展趋势。在这种趋势下数据中心的业务复杂性增加，而这种复杂性也为数据中心的安全体系引入许多不确定因素，一些未实施正确安全策略的数据中心，黑客和蠕虫将顺势而入。

当前数据中心面对的主要安全威胁包括。

(1）面向应用层的攻击。

常见的应用攻击包括恶意蠕虫、病毒、缓冲溢出代码、后门木马等。应用攻击的共同特点是利用了软件系统在设计上的缺陷，并且他们的传播都基于现有的业务端口，因此应用攻击可以毫不费力地躲过那些传统的或者具有少许深度检测功能的防火墙。国际计算机安全协会 ICSA 实验室调查的结果显示，2005 年病毒攻击范围提高了 39%，重度被感染者提高了 18%，造成的经济损失提高了 31%。尤为引人注意的是，跨防火墙的应用层(ISO 7 层)攻击提高了 278%，即使在 2004 年，这一数字也高达 249%。

(2）面向网络层的攻击。

除了由于系统漏洞造成的应用攻击外，数据中心还要面对拒绝服务攻击(DoS)和分布式拒绝服务攻击(DDoS)的挑战。DoS/DDoS 是一种传统的网络攻击方式，然而其破坏力却十分强劲。据 2004 年 美国 CSI/FBI 的计算机犯罪和安全调研分析，DoS 和 DDoS 攻击已成为对企业损害最大的犯罪行为，超出其他各种犯罪类型两倍。DoS/DDoS 攻击大行其道的原因主要是利用了 TCP/IP 的开放性原则，从任意源地址向任意目标地址都可以发送数据包。DoS/DDoS 利用看似合理的海量服务请求来耗尽网络和系统的资源，从而使合法用户无法得到服务的响应。

2）数据中心安全建设思路

数据中心安全解决方案的思路可用十二个字概括：三重保护、多层防御；分区规划，分层部署。

(1）三重保护，多层防御。

从“数据中心服务器资源”向外延伸有三重保护。

① 具有丰富安全特性的交换机构成数据中心网络的第一重保护。

② 具有高性能检测引擎的 IPS 对网络报文做深度检测，构成数据中心网络的第二重保护。

③ 凭借高性能硬件防火墙构成的数据中心网络边界，对数据中心网络做第三重保护。

用一个形象的比喻来说明数据的三重保护：数据中心就像一个欣欣向荣的国家，来

往的商客就像访问数据中心的报文;防火墙是驻守在国境线上的军队,一方面担负着守卫国土防御外族攻击(DDoS)的重任,另一方面负责检查来往商客的身份(访问控制);IPS是国家的警察,随时准备捉拿虽然拥有合法身份,但仍在从事违法乱纪活动的商客(蠕虫、病毒),以保卫社会秩序;具有各种安全特性的交换机就像商铺雇佣的保安,提供最基本的安全监管,时刻提防由内部人员造成的破坏(STP攻击)。

三重保护为数据中心网络提供了从链路层到应用层的多层防御体系。交换机提供的安全特性构成安全数据中心的网络基础,提供数据链路层的攻击防御。数据中心网络边界安全定位在传输层与网络层的安全上,通过状态防火墙可以把安全信任网络和非安全网络进行隔离,并提供对DDoS和多种畸形报文攻击的防御。IPS可以针对应用流量做深度分析与检测能力,既可以有效检测并实时阻断隐藏在海量网络流量中的病毒、攻击与滥用行为,也可以对分布在网络中的各种流量进行有效管理,从而达到对网络应用层的保护。

(2) 分区规划,分层部署。

在数据中心网络中存在不同价值和易受攻击程度不同的设备,按照这些设备的情况制定不同的安全策略和信任模型,将网络划分为不同区域,这就是所谓的分区思想。数据中心网络根据不同的信任级别可以划分为:远程接入区、局域网、Internet服务器区、Extranet服务器区、Intranet服务器区、管理区、核心区。

### 5. 全局安全管理解决方案

参与了大量网络安全建设实践后可以了解,除了在信息传输流程中实施安全解决方案之外,还需要进行全局安全管理,这种管理涉及到网络上的设备、使用者以及业务,只有对这三者实现闭环管理,才能对网络安全状况了如指掌。因此,大型企业系统建设一个“全局安全管理平台”是必要的。

对于网络系统来说,安全入侵经常将网络作为一个整体而不仅是针对某一个子系统。一个安全攻击事件可能是独立的,也可能是一个较大规模协同攻击的一部分。对于所有的安全检测点,如果没有一个集中的分析视角,可能低估某个安全攻击的真正威胁,相应采取的安全措施也可能无法解决真正的问题。因此,对系统所记录和存储的审计数据进行综合分析及处理至关重要。这些审计数据可能来自防火墙、路由器、入侵防御系统、主机系统、防病毒系统和桌面安全系统。对上述审计数据的统一和集中的分析将能帮助更好地管理安全事件,从而描绘出整个系统当前安全情况的更清晰和准确的图画。同时,通过集中管理,一个企业可以最大程度地减少重复工作从而提高安全事件管理的效率。

1) 全局安全管理解决方案概述

当前,大型企业系统安全管理中遇到的问题包括如下几点。

(1) 对实时安全信息不了解,无法及时发出预警报告。

(2) 各种安全设备是孤立的,无法相互关联,信息共享。

(3) 安全事件发生以后,无法及时诊断网络故障的原因,恢复困难。

(4) 网络安全专家匮乏,没有足够的人员去监控、分析、解决问题。

全局安全管理平台旨在集中部署网络安全防护策略,简化对安全部件的管理,确保网络安全策略的统一。广泛采集与分析来自于计算机、网络、存储、安全等设施的告警事件,通过关联来自于不同地点、不同层次、不同类型的安全事件,发现真正的安全风险,提高安全报警的信噪比。准确、实时地评估当前的网络安全态势和风险,并根据预先制定的策略做出快速响应。全网安全管理解决原理框架如图 8-18 所示。

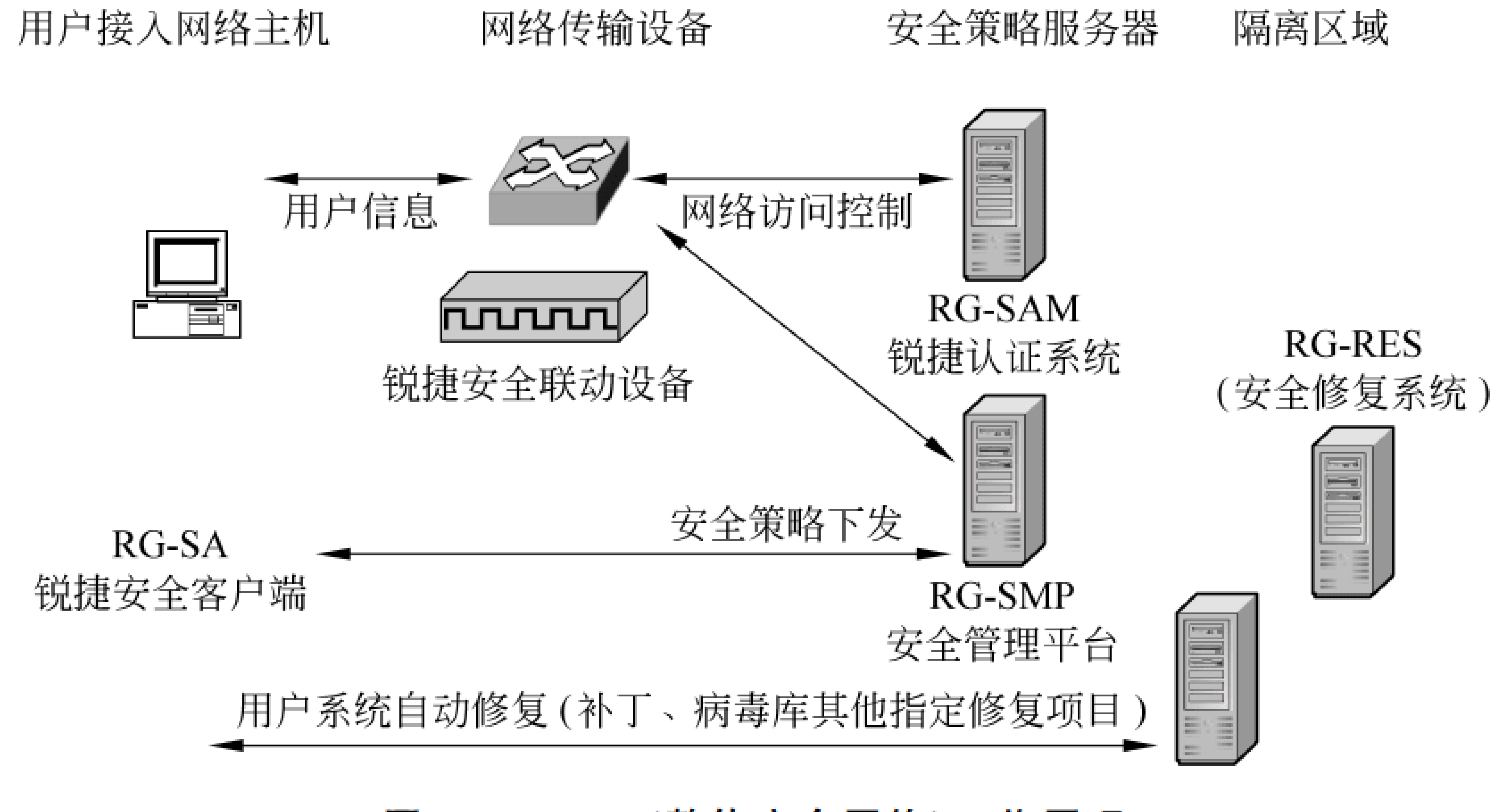



**图 8-18　GSN(整体安全网络)工作原理**

2）安全策略的集中部署

网络中的安全部件涉及身份安全、终端安全、设备安全、连接安全、网络安全等各个层面,对应的安全防护技术包括 AAA、防病毒、漏洞检测、防火墙、VPN、IPS 等不同层次的防御部件。集中部署各部件的安全防护策略,可以简化对安全部件的管理,确保网络安全策略的统一,提高安全管理工作的效率。全局安全管理平台的安全策略集中部署提供了集成、统一、完整的安全防护策略配置功能,可以通过直观的网络、服务器、终端及用户拓扑图,查看和配置安全策略。

3）安全事件的深度感知

网络的不同层次、不同节点往往都部署了相应的安全部件,分别起到不同层面的安全防御作用。为了实时、全面地获取网络安全信息,必须解决网络安全管理中的事件透明性问题,让管理员可以监控到网络中每个设备的运行状态,为网络安全分析与决策提供支持。全局安全管理平台可以收集来自不同部件的安全事件数据,如异常登录事件、异常操作事件、漏洞检测事件、系统资源异常占用事件、流量异常事件等,帮助管理员及时掌握网络中设备和终端的安全状态,为进一步的深入分析和决策奠定准确的数据基础。

4）安全事件的关联分析

网络中的各种安全部件产生的众多安全事件,往往使管理员淹没于信息的海洋中。各安全部件本身的局限性造成的误报和漏报,容易导致真正的攻击被忽视。全局安全管理平台在全面采集安全事件的基础上,通过各种基于统计和规则的关联分析算法,结合安全事件产生的网络环境、资产重要程度、系统漏洞级别,对安全事件进行深度分析,可以有效提高安全事件的信噪比,减少告警日志数量而不丢失重要信息,为安全事件审计和风险响应提供更准确的决策支持。

5）安全威胁的协同响应

对安全事件进行全面采集和关联分析的目的是准确地阻断和防止攻击。全局安全管理平台在全面了解网络资源部署的条件下，可以根据攻击源的不同，智能选择控制点以更有效地防止攻击。例如对于外部攻击选择在防火墙的 ACL 阻断、对内部攻击选择用户接入交换机的端口关闭、对于内部蠕虫爆发选择隔离攻击源。也可以针对不同的被攻击对象，区分响应方式，以提高整个网络的自防御能力，例如对于用户终端可以强制进行补丁修复和病毒库升级，对于服务器资源可以动态更新安全配置。

高效的安全解决方案不仅仅在于当安全事件发生时，能够迅速察觉、准确定位，更重要的是能够及时制定合理的、一致的、完备的安全策略，并最大限度地利用现有网络安全资源，通过智能分析和协同响应及时应对各种真正的网络攻击。全局安全管理解决方案为实现这一目标而构建了开放的、可持续演进的安全管理平台，通过对防护、检测和响应等不同生命周期的各个安全环节进行基于策略的管理，将各种异构的安全设备、网络设备、用户终端和管理员有机的连接起来，构成了一个智能的、联动的闭环响应体系，可在保护现有网络基础设施投资的基础上有效应对新的安全威胁、大幅提升对大型企业系统业务的安全保障。

大型企业网络安全整体解决方案如图 8-19 所示。

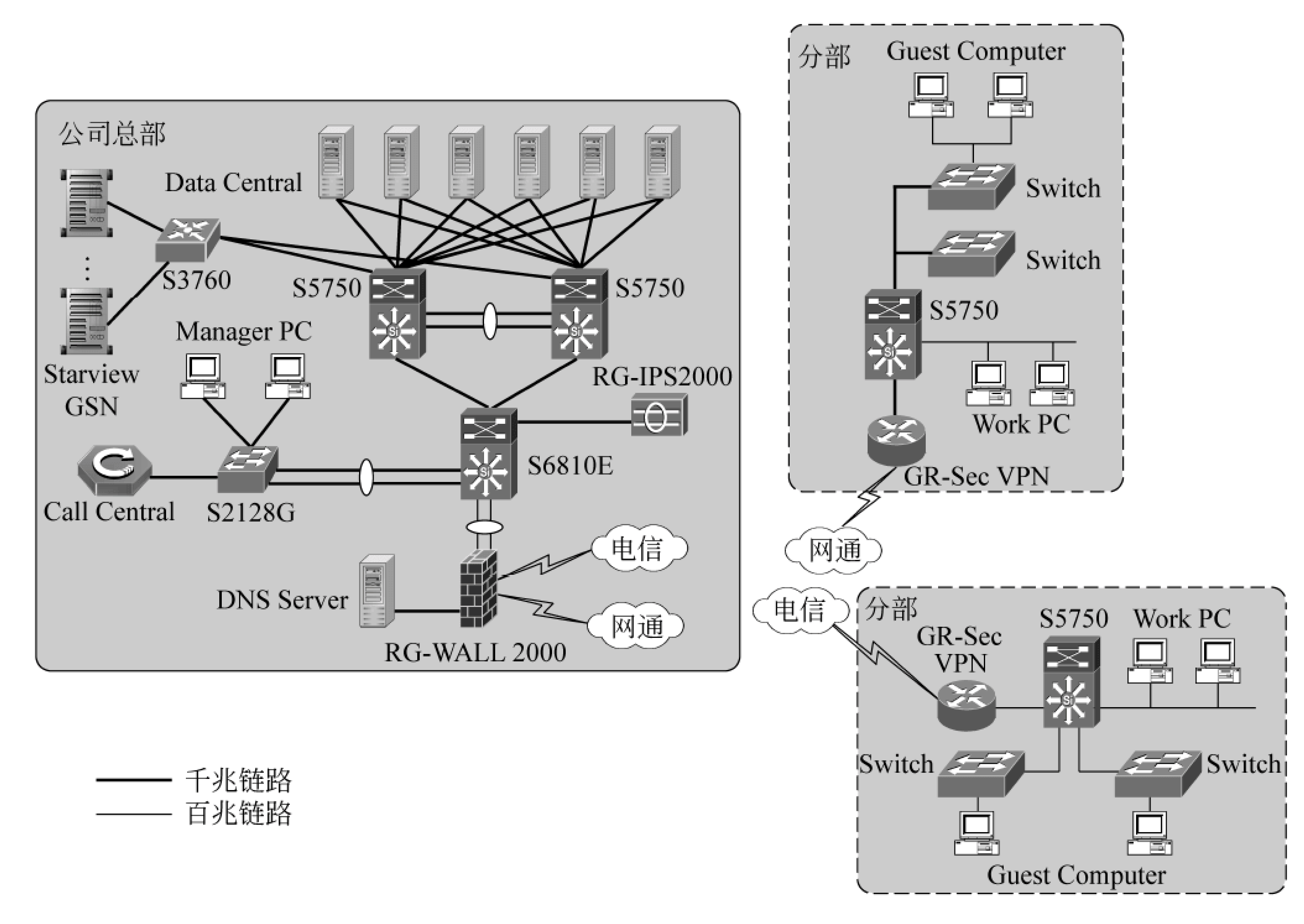



图 8-19　大型企业网络安全解决方案

## 8.3.3 银行业务系统安全体系

与早期的集中式应用不同的是，现在的银行业务系统大多基于客户机/服务器模式

和 Internet/Intranet 网络计算模式的分布式应用。在这样的环境中,企业的数据库服务器、电子邮件服务器、WWW 服务器、文件服务器、应用服务器等都是供用户出入的“门户”,只要有一个“门户”没有完全保护好,“黑客”就会通过这道门进入系统,窃取或破坏所有资源。绝对安全与可靠的信息系统并不存在,一个所谓的安全系统实际上应该是“使入侵者花费不可接受的时间与金钱,并且承受很高的风险才能闯入”。安全是个过程而不是目的,安全的努力依赖于许多因素,例如职员的调整、新业务应用的实施、新攻击技术与工具的导入和安全漏洞评估。银行业务系统的安全分为网络安全、系统安全、用户安全、应用与服务安全、数据安全 5 个部分。银行业务系统的安全体系如图 8-20 所示。




**图 8-20 银行业务系统的安全体系**

其中网络安全包括查明任何非法访问或偶然访问的入侵者,保证只有授权许可的通信才可以在客户机和服务器之间建立连接,而且正在传输中的数据不能被读取和改变。系统安全包括控制访问服务器,防止病毒的侵入,检测有意或偶然闯入系统的不速之客。风险评估被用来检查系统安全配置的缺陷,发现安全漏洞。政策审查则用来监视系统是否严格执行了规定的安全政策。用户安全是管理用户账户,在用户获得访问特权时设置用户功能,或在他们的访问特权不再有效时,限制用户账户。身份验证用来确保用户的登录身份与其真实身份相符,并对其提供单点注册,以解决多个密码的问题。应用与服务安全是指对应用程序和服务的密码和授权的管理,大多数应用程序和服务都是靠密码保护的,加强密码变化是安全方案中必不可少的手段,而授权则是用来规定用户对系统的访问权限。数据安全是保持数据的保密性和完整胜,保证非法或好奇者无法阅读它。数据完整性是指防止非法或偶然的数据改动现代计算机网络系统的安全隐患隐藏在系统的各个角落。所以对系统安全管理应该是多层次、多方面的,要从网络、操作系统、应用各个方面提高系统的安全级别,还要把原来由使用人员维护的安全规则让计算机系统自动实现,以加强系统的总体安全性。对系统安全的管理和维护需要各种层次的安全专家才能完成。因此,对系统安全的管理应该由 70%的规则和方法加 30%的产品和技术组成。这些规则和方法包括风险评估、安全策略、强大的审计手段等。另外,IT 系统的结构变化、应用系统的变化都会导致安全策略的变化,因此上述过程不是静态的,而是周而复始的过程,该过程在维护系统安全的活动中一直存在。

本章从整体安全的角度出发,完整地论述了网络安全系统的框架、网络安全系统设计的基本原则以及基本方法,并在对典型行业所面对的网络安全问题,系统地分析了解决思路,给出了较为完整成熟的解决方案。同时,针对无线网络的特殊性,在论述了无线网络工作原理的基础上,阐述了无线网络由于工作机理造成的网络安全的特殊问题,单

独提出了无线网络安全解决方案。

# 习 题 8

## 1. 填空题

(1) 网络安全风险有五个层次,即________、________、________、________和________。

(2) 网络安全管理的目标主要包括________、________、________、________、________和________6 个方面。

(3) 制定网络安全策略的总体原则是________、________、________和具体应考虑________、________和________。

(4) 网络安全的特征应具有保密性、________、________和________4 个方面的特征。

## 2. 问答题

(1) 为什么人为因素是影响网络安全的最主要因素?

(2) 无线网络主要有哪些安全威胁?

(3) WEP 主要有哪些安全漏洞?

(4) 从网络管理员的角度,简述企事业单位内部网络应采取的各种安全策略。

(5) 目前网络安全解决方案有哪些?

# 参 考 文 献

1. 哈根. Linux Server Hacks(卷二)100个业界最尖端的技巧和工具. 北京：清华大学出版社，2007
2. 赵小林. 网络安全技术教程. 北京：国防工业出版社，2006
3. Gert De Laet、Gert Schauwers. Network Security Fundamentals. 张耀疆、李磊译. 北京：人民邮电出版社，2006
4. 中国计算机学会学术工作委员会. 中国计算机科学技术发展报告 2005. 北京：清华大学出版社，2006
5. 邓志华等. 网络安全与实训教程. 北京：人们邮电出版社，2005
6. 辜川毅. 计算机网络安全技术. 北京：机械工业出版社，2005
7. 沈苏彬. 网络安全原理与应用. 北京：人民邮电出版社，2005
8. 陈志雨. 计算机信息安全技术应用. 北京：电子工业出版社，2005
9. 余成波. 计算机网络安全技术. 北京：北京工业大学出版社，2005
10. Roberta Bragg、Mark Rhodes-Ousley. 完全手册丛书网络安全完全手册. 北京：电子工业出版社，2005
11. Sean Convery. 网络安全体系结构. 北京：人民邮电出版社，2005
12. 顾新光等. 计算机网络安全技术与应用. 北京：科学出版社，2005
13. 连一峰. 网络攻击原理与技术. 北京：科学出版社，2004
14. 李涛等. 网络安全概论. 北京：电子工业出版社，2004
15. 蔡皖东. 网络与信息安全. 西安：西北工业大学出版社，2004
16. 张玉清. 网络安全扫描技术. 北京：清华大学出版社，2004
17. 唐正军. 入侵检测技术. 北京：清华大学出版社，2004
18. 潘志翔. 黑客攻防编程解析. 北京：机械工业出版社，2003
19. 麦伍德. 网络安全实用教程. 北京：清华大学出版社，2003
20. Eric Maiwald. 网络安全实用指南. 北京：清华大学出版社，2003
21. 姚顾波. 黑客终结—网络安全完全解决方案. 北京：电子工业出版社，2003
22. Seth Foge，Cyrus Peikari. Windows Internet 黑客防范与安全策略. 北京：清华大学出版社，2002
23. 袁家政. 计算机网络安全与应用技术. 北京：清华大学出版社，2002
24. 谭晓. 电子商务的安全策略. 呼和浩特：内蒙古科技与经济，2007 年第 8 期
25. 张震. E-mail 的安全问题与保护措施. 福州：福建电脑，2007 年第 9 期
26. 邱伟江. 基于校园网络的电子邮件安全策略研究. 兰州：甘肃科技，2005 年第 11 期
27. 马建林. 电子商务安全策略问题研究. 北京：中国科技信息，2005 年第 17 期
28. 肖道举. Web 服务安全保障机制研究. 武汉：华中科技大学学报，2004 年第 4 期

# 高等院校信息技术规划教材

## 系 列 书 目

| 书 名 | 书 号 | 作 者 |
| --- | --- | --- |
| 数字电路逻辑设计 | 978-7-302-12235-7 | 朱正伟 等 |
| 计算机网络基础 | 978-7-302-12236-4 | 符彦惟 等 |
| 微机接口与应用 | 978-7-302-12234-0 | 王正洪 等 |
| XML 应用教程(第 2 版) | 978-7-302-14886-9 | 吴 洁 |
| 算法与数据结构 | 978-7-302-11865-7 | 宁正元 等 |
| 算法与数据结构习题精解和实验指导 | 978-7-302-14803-6 | 宁正元 等 |
| 工业组态软件实用技术 | 978-7-302-11500-7 | 龚运新 等 |
| MATLAB 语言及其在电子信息工程中的应用 | 978-7-302-10347-9 | 王洪元 |
| 微型计算机组装与系统维护 | 978-7-302-09826-3 | 厉荣卫 等 |
| 嵌入式系统设计原理及应用 | 978-7-302-09638-2 | 符意德 |
| C ++ 语言程序设计 | 978-7-302-09636-8 | 袁启昌 等 |
| 计算机信息技术教程 | 978-7-302—09961-1 | 唐 全 等 |
| 计算机信息技术实验教程 | 978-7-302—12416-0 | 唐 全 等 |
| Visual Basic 程序设计 | 978-7-302-13602-6 | 白康生 等 |
| 单片机 C 语言开发技术 | 978-7-302-13508-1 | 龚运新 |
| ATMEL 新型 AT89S52 系列单片机及其应用 | 978-7-302-09460-8 | 孙育才 |
| 计算机信息技术基础 | 978-7-302-10761-3 | 沈孟涛 |
| 计算机信息技术基础实验 | 978-7-302-13889-1 | 沈孟涛 著 |
| C 语言程序设计 | 978-7-302-11103-0 | 徐连信 |
| C 语言程序设计习题解答与实验指导 | 978-7-302-11102-3 | 徐连信 等 |
| 计算机组成原理实用教程 | 978-7-302-13509-8 | 王万生 |
| 微机原理与汇编语言实用教程 | 978-7-302-13417-6 | 方立友 |
| 微机组装与维护用教程 | 978-7-302-13550-0 | 徐世宏 |
| 计算机网络技术及应用 | 978-7-302-14612-4 | 沈鑫剡 等 |
| 微型计算机原理与接口技术 | 978-7-302-14195-2 | 孙力娟 等 |
| 基于 MATLAB 的计算机图形与动画技术 | 978-7-302-14954-5 | 于万波 |
| 基于 MATLAB 的信号与系统实验指导 | 978-7-302-15251-4 | 甘俊英 等 |
| 信号与系统学习指导和习题解析 | 978-7-302-15191-3 | 甘俊英 等 |
| 计算机与网络安全实用技术 | 978-7-302-15174-6 | 杨云江 等 |
| Visual Basic 程序设计学习和实验指导 | 978-7-302-15948-3 | 白康生 等 |
| Photoshop 图像处理实用教程 | 978-7-302-15762-5 | 袁启昌 等 |
| 数据库与 SQL Server 2005 教程 | 978-7-302-15841-7 | 钱雪忠 著 |
| 计算机网络实用教程 | 978-7-302-16212-4 | 陈 康 等 |

# 读者意见反馈

亲爱的读者：

感谢您一直以来对清华版计算机教材的支持和爱护。为了今后为您提供更优秀的教材，请您抽出宝贵的时间来填写下面的意见反馈表，以便我们更好地对本教材做进一步改进。同时如果您在使用本教材的过程中遇到了什么问题，或者有什么好的建议，也请您来信告诉我们。

地址：北京市海淀区双清路学研大厦 A 座 602 室　计算机与信息分社营销室 收

邮编：100084　　电子邮件：jsjjc@tup.tsinghua.edu.cn

电话：010-62770175-4608/4409　　邮购电话：010-62786544

教材名称：计算机网络安全实用技术

ISBN：978-7-302-17966-5

**个人资料**

姓名：________________ 年龄：_______ 所在院校/专业：_____________________

文化程度：____________ 通信地址：_______________________________________

联系电话：____________ 电子信箱：_______________________________________

**您使用本书是作为：**□指定教材 □选用教材 □辅导教材 □自学教材

**您对本书封面设计的满意度：**

□很满意 □满意 □一般 □不满意　改进建议_______________________________

**您对本书印刷质量的满意度：**

□很满意 □满意 □一般 □不满意　改进建议_______________________________

**您对本书的总体满意度：**

从语言质量角度看 □很满意 □满意 □一般 □不满意

从科技含量角度看 □很满意 □满意 □一般 □不满意

**本书最令您满意的是：**

□指导明确 □内容充实 □讲解详尽 □实例丰富

**您认为本书在哪些地方应进行修改？（可附页）**

________________________________________________________________________

________________________________________________________________________

**您希望本书在哪些方面进行改进？（可附页）**

________________________________________________________________________

________________________________________________________________________

# 电子教案支持

敬爱的教师：

为了配合本课程的教学需要，本教材配有配套的电子教案（素材），有需求的教师可以与我们联系，我们将向使用本教材进行教学的教师免费赠送电子教案（素材），希望有助于教学活动的开展。相关信息请拨打电话 010-62776969 或发送电子邮件至 jsjjc@tup.tsinghua.edu.cn 咨询，也可以到清华大学出版社主页（http://www.tup.com.cn 或 http://www.tup.tsinghua.edu.cn）上查询。